

Proceedings of the First International Seminar

ACTES

des Premières Journées Internationales

ACSA'90

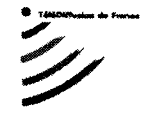
ACCÈS CONDITIONNEL AUX SERVICES AUDIOVISUELS

CONDITIONAL ACCESS FOR AUDIOVISUAL SERVICES

RENNES 12 – 13 – 14 JUIN 1990
(France)











ACSA

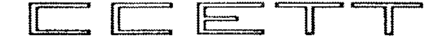
Proceedings of the First International Seminar

ACTES
des Premières Journées Internationales
ACSA'90

ACCÈS CONDITIONNEL AUX SERVICES AUDIOVISUELS

CONDITIONAL ACCESS FOR AUDIOVISUAL SERVICES

RENNES 12 – 13 – 14 JUIN 1990
(France)









COMITÉ INTERNATIONAL DE PROGRAMME
INTERNATIONAL PROGRAMME COMMITTEE

PRÉSIDENT/*CHAIRMAN* :

Jacques PONCIN (CCETT)

MEMBRES/*MEMBERS* :

Michel AYEL (RPIC)
Joseph BLINEAU (Thomson CE)
Jean-Pierre COUSTEL (France Telecom STI)
Louis GUILLOU (CCETT)
Joseph HASCOET (MatraCommunication)
Marc LASSUS (Gemplus)
Mark MEDRESS (General Instrument Corporation)
Graham MILLS (BT Vision)
Bjorn PERSSON (Scansat)
Jean-Jacques QUISQUATER (Philips Research Lab)
Michel RENERIC (TDF)
Charles SANDBANK (BBC Research)
Kjell STÅHLBOM (Nokia Luxor)
Michel UGON (Bull CP8)

COMITÉ D'ORGANISATION
ORGANISING COMMITTEE

F. SCARABIN – V. MICHON (CCETT)

Secrétariat **ACSA'90**
CCETT
4, rue du Clos Courtel – BP 59
35512 CESSON-SÉVIGNÉ Cédex – FRANCE
Tél : (+33) 99 02 41 98
Télécopie (+33) 99 02 40 98 - Télex : 740284 F

SOMMAIRE

ARCHITECTURE DE SYSTÈMES I
Président de session : Y. GUINET (RPIC)

ARCHITECTURE DE SYSTÈMES II
Président de session : CH. BENNETT (General Instrument Corp.)

CARTES À PUCE

Président de session : P. MAES (GEMPLUS)

POINT DE VUE DES OPÉRATEURS

Président de session : B. PERSSON (SCANSAT)

ÉQUIPEMENTS TERMINAUX

Président de session : V. MICHON (CCETT)

INDEX DES NOMS D'AUTEURS



LA PREMIÈRE DÉCENNIE DES SERVICES AUDIOVISUELS À ACCÈS CONDITIONNEL EN FRANCE

Jean-Pierre **LANDRAGIN**
La Radiotechnique Portenseigne
24 quai Galliéni
92156 SURESNES Cedex
FRANCE
Tél : +33 (1) 40 99 62 89

Philippe **MEILLAN**
Télédiffusion de France
21-27 rue Barbès
92120 MONTROUGE
FRANCE
Tél : +33 (1) 49 65 19 68

TABLE DES MATIÈRES

1. INTRODUCTION

A la suite des recherches des centres d'études publics et plus spécialement du CCETT, les services audiovisuels à accès conditionnel se sont progressivement développés sur plus d'une décennie, sous l'impulsion des opérateurs publics et privés, dont TDF, et avec la contribution déterminante de la Radiotechnique Portenseigne.

Les différentes étapes de ces contributions sont les suivantes :

Antiope USA [1-1]
Antiope embrouillé [1-2]
Carte à mémoire PCO pour Antiope embrouillé [1-3]
Carte à mémoire PC1 pour télévision embrouillée [1-4]
Contrat retard variable [1-5]
Contrat décalage circulaire [1-6]
Contrat récepteur de référence D2MAC [1-7]
Contrat contrôle d'accès D2MAC [1-8] [1-9]
Marché D2MAC-Eurocrypt [1-10]

Partant des préliminaires des systèmes de diffusion d'images et de données à accès conditionnel et intégrant un nouveau procédé de codage des signaux de couleur, ainsi que les récents progrès dans le traitement du son de haute qualité, les systèmes de la famille MAC, particulièrement DMAC et D2MAC constituent les signaux de télévision les plus complets qu'on puisse imaginer à l'heure actuelle, dans la mesure où ils contiennent intrinsèquement tout ce qui est nécessaire à assurer ultérieurement toutes les fonctions que l'opérateur, même le plus imaginatif dans le domaine de la commercialisation des services à valeur ajoutée, pourra être amené à demander. Nous allons montrer dans ce qui suit que ce n'est que l'aboutissement inéluctable de la mise en oeuvre systématique et poussée à l'extrême des techniques et technologies maximales nécessaires à la réalisation du meilleur système de télévision à accès conditionnel, et que c'est finalement la télévision cryptée qui a ouvert la porte à la haute définition à la mode européenne en initiant, en stimulant, en entraînant les recherches et applications nécessaires et en mettant en pratique avec plus ou moins de bonheur les résultats obtenus.

2. EMBROUILLAGE ET TRAITEMENT DU SIGNAL VIDEO

Divers procédés d'embrouillage du signal d'image sont en usage depuis des années dans le monde et font appel à des procédés de traitement de nature analogique (inversion de la polarité de luminance ou suppression d'impulsions de synchronisation, introduction de signaux ou de filtrages parasites).

Des études concernant les dispositifs d'accès conditionnel par embrouillage d'émissions de télévision en France ont été amorcées par le CCETT dès 1977, et testées pour la première fois en 1980. Outre l'inversion de polarité de ligne, l'embrouillage d'image concernait des procédés de modifications temporelles du signal. Ces méthodes de traitement ne peuvent donc s'appliquer qu'aux signaux en bande de base et impliquent donc la démodulation préalable de l'émission de télévision à décoder. L'insertion du "décodeur" (désembrouilleur) nécessitait l'implantation sur les récepteurs d'un connecteur de "péritélévision" normalisé [2-1].

Les principes de modifications temporelles nécessitent la capacité de mémoriser certaines parties du signal vidéo. Aussi, une fois épuisées les ressources de technologies dérivées des procédés analogiques (lignes à retard, dispositifs à couplage de charges...), la mise en oeuvre de ces types d'embrouillages mène tout naturellement à l'utilisation des techniques numériques.

Le principe de l'inversion de polarité vidéo ayant rapidement montré ses limites, deux procédés avaient été étudiés simultanément : le procédé à retard variable dit Discret 1 et le procédé à segmentation de lignes ou décalage circulaire dit Discret 2 [2-2] dont des variantes furent ultérieurement envisagées [2-3][2-4].

Les premiers matériels réalisant les codages Discret 1 et Discret 2 furent réalisés sur marché TDF [2-5] au LEP* au tout début de la décennie 80 [2-6].

---

* Laboratoire d'Electronique et de Physique Appliquée - 3, Avenue Descartes - 94450 Limeil-Brévannes (Actuellement Laboratoire d'Electronique PHILIPS)

Toutefois, les technologies numériques disponibles à cette époque ne permettaient pas la réalisation d'un décodeur grand-public viable. Les matériels disponibles dès 1982 étaient volumineux, lourds et générateurs de nombreuses calories.

. La conséquence a été l'adoption par Canal + du décodeur Discret 11 en technologie analogique, faisant appel à des lignes à retard [2-7]. L'ensemble d'embrouillage réalisé par CIT-Alcatel pour la même application utilisait quant à lui des technologies professionnelles (convertisseurs TRW et cartes logiques TTL).

. Toutefois, les études concernant la réalisation industrielle d'un décodeur Discret 2 continuaient [2-8]. Elles aboutirent au développement de composants spécifiques, en particulier des convertisseurs destinés au marché grand-public [TDA 5702 et 5703] firent leur apparition en 1985 [2-9] dans le groupe PHILIPS.

Dans ce jeu de circuits intégrés, réalisés pour le même marché TDF, on trouvait aussi un générateur pseudo-aléatoire non linéaire à 20 bits (structure de Geffe), TDA 5707 [2-10], avec le circuit de génération des signaux de service associés (TDA 5704) et les circuits de pilotage des adresses des mémoires RAM (TDA 5705 et 5706).

. Le premier décodeur grand public à technologie numérique, Discret 12, a fait son apparition en 1985. Il reprenait les circuits TDA 5702 et TDA 5703, et traitait les signaux en retard variable au moyen d'un "Gate Array" et d'un microcontrôleur "RT 86". Il était initialement destiné aux marchés internationaux [2-11], associé à un embrouilleur ALCATEL dérivé du matériel développé pour CANAL+. Il a aussi été utilisé par l'administration française [2-12]**, associé, soit à l'embrouilleur ALCATEL, soit à l'embrouilleur VSE 01 développé par la Radiotechnique Industrielle et Commerciale à partir de 1986.

Enfin, l'appareil TUDI 12, incorporant un ensemble de réception à synthèse de fréquence a remporté un succès considérable sur les marchés internationaux [2-13].

. L'embrouillage des images selon le procédé Discret 2 n'est devenu économiquement viable que récemment, grâce à la baisse du coût des composants (convertisseurs, mémoires), à l'intégration à grande échelle et surtout au développement des possibilités en circuits spécifiques (ASIC).

---

* Tel quel ou sous sa forme "professionnelle" TDR12 (tête de réseau).

Les éléments stratégiques et critiques, notamment le convertisseurs, ont vu leur prix chuter dans des proportions importantes et leurs défauts d'origine ont pour la plupart été réduits à un niveau tolérable en production industrielle. On peut citer, outre les produits originaires du groupe Philips (TDA 8702, 8703, 8708), les composants ITT (UVC 3100, 3101...) dont l'usage de plus en plus fréquent dans les téléviseurs à châssis numérique assure la pérennité à des coûts acceptables pour des produits grand-public.

Pendant ce temps, PHILIPS apportait l'embrouillage par décalage circulaire au fonds commun du D2MAC [2-14].

On peut remarquer que toutes les techniques nécessaires à la formation du signal image MAC étaient déjà identifiées et la plus grande partie utilisées :

. Utilisation de mémoires vives écrites à un rythme et lues à un rythme différent et/ou en temps différé.

. Ecritures ou lectures non-linéaires.

. Mise en forme de transitions ou interpolations.

Par ailleurs, un certain nombre de difficultés avaient été identifiées à l'époque ; certaines étant résolues à l'heure actuelle, d'autres n'ayant toujours pas trouvé de solution :

. Nécessité de disposer d'une excellente synchro (d'où la synchro "numérique" adoptée en MAC).

. Sensibilité aux perturbations apportées par la diffusion terrestre : échos, line tilt .... [2-15]

3. ACCES CONDITIONNEL ET DIFFUSION DE DONNEES

Ainsi qu'on l'a vu précédemment, la mise en oeuvre de l'accès conditionnel s'associe particulièrement bien à l'utilisation des techniques numériques.

Or les techniques de diffusion numériques se sont introduites en France, de même que dans toute l'Europe de l'Ouest à travers le télétexte et la diffusion de données.

En France le télétexte n'a pas été conçu comme un simple service complémentaire des programmes de télévision mais comme un service autonome devant trouver son équilibre économique et par conséquent un mode de financement propre.

C'est ainsi qu'il a été imaginé de financer les magazines de télétexte par le paiement d'abonnements. Percevoir des abonnements sur un service diffusé nécessite de disposer des moyens d'en restreindre l'accès aux usagers autorisés ; les études conduites alors, parallèlement aux premiers travaux sur la télévision à péage, ont rapidement conduit à la conclusion que cela passait par les notions d'embrouillage et de contrôle des titres d'accès :

. Embrouillage : c'est-à-dire modification du signal de telle sorte à le rendre incompréhensible à celui qui ne dispose pas de titres d'accès,

. Contrôle des titres d'accès : c'est-à-dire mise à disposition de moyens permettant de vérifier que les usagers ont bien acquis les droits d'accès aux programmes.

La technique d'embrouillage retenue a consisté à faire intéragir le signal avec une séquence pseudo-aléatoire initialisée par un mot de contrôle.

Les principales notions qui se sont alors dégagées ont été les suivantes :

. Utilisation d'un générateur pseudo-aléatoire de grande dimension (séquence pseudo-aléatoire longue) avec mot de contrôle de grande taille (60 bits). En fait, le dispositif utilisé était un Générateur d'octets chiffrants (GOC) adapté au traitement par un microprocesseur et dont le comportement était analogue à celui d'un Générateur Pseudo-Aléatoire.

. Renouvellement du mot de contrôle à rythme fréquent et modification encore plus fréquente de la séquence pseudo-aléatoire, un élément variable du signal intervenant dans son initialisation,

- Utilisation d'un système non pas à distribution des mots de contrôle mais à distribution d'autorisations, une autorisation comportant d'une part des titres d'accès et d'autre part une clé d'accès permettant, par le biais d'un algorithme cryptographique, de reconstituer le mot de contrôle, diffusé sous forme chiffrée (cryptogramme),

- Variété des modes d'accès aux programmes :

  Abonnement durée fixe ou variable,
  Paiement à la séance prévalidée ou télévalorisée (possibilité de choix impulsif).

- Diffusion des données de contrôle des titres d'accès sous la forme de messageries de contrôle d'accès multiplexées avec le signal.

- Banalisation du terminal de réception qui ne comporte aucun secret et aucun élément de personnalisation, ceux-ci étant contenus dans un support de titres d'accès détachable qui a été réalisé sous la forme d'une carte à micro-circuit.

Ces notions ont trouvé leur concrétisation :

- Dans le système d'accès conditionnel défini pour le télétexte ANTIOPE et dont la spécification a été publiée en 1984 [3-1],

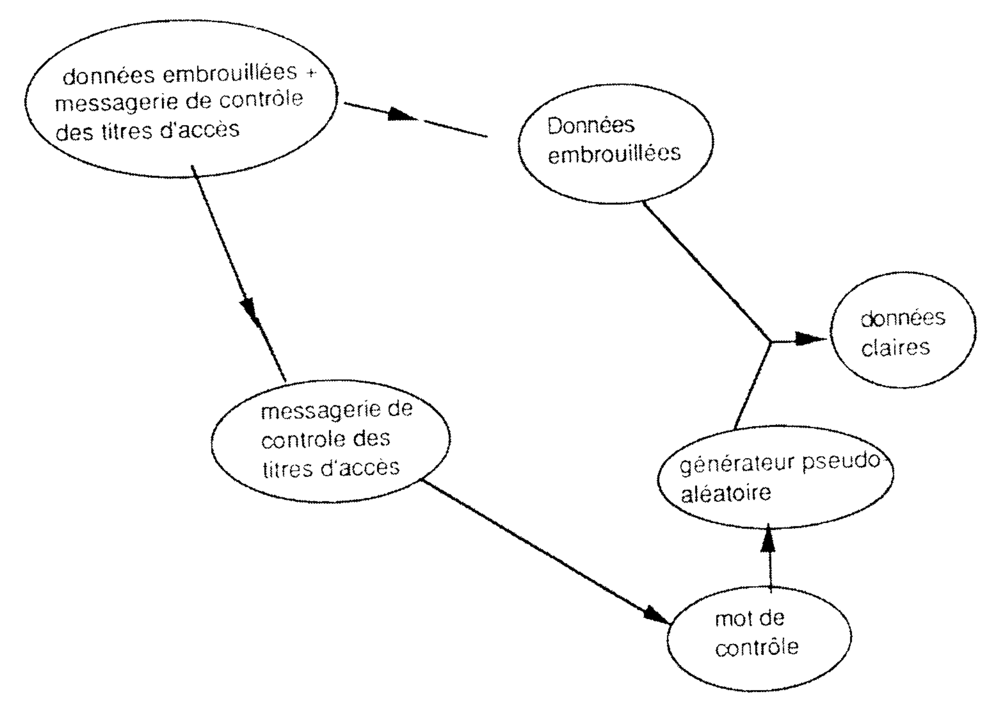
- Dans le développement de la première carte à mémoire support de titres d'accès, la carte porte-clés PCO [3-2],

- Dans la reconnaissance des principes généraux ainsi définis comme base de l'accès conditionnel aux services audiovisuels par la normalisation internationale à travers le rapport 1079 du CCIR adopté en 1986 [3-3].

Le système d'accès conditionnel défini pour le télétexte ANTIOPE reposait donc à la fois sur la diffusion de messageries de contrôle des titres d'accès et l'utilisation d'un support de titres d'accès détachable, ainsi que sur les notions d'autorisation et de distribution d'autorisation. La distribution d'autorisation s'effectuait par valorisation des supports de titres d'accès sur un terminal, soit dans un centre de gestion, soit via un service videotex.

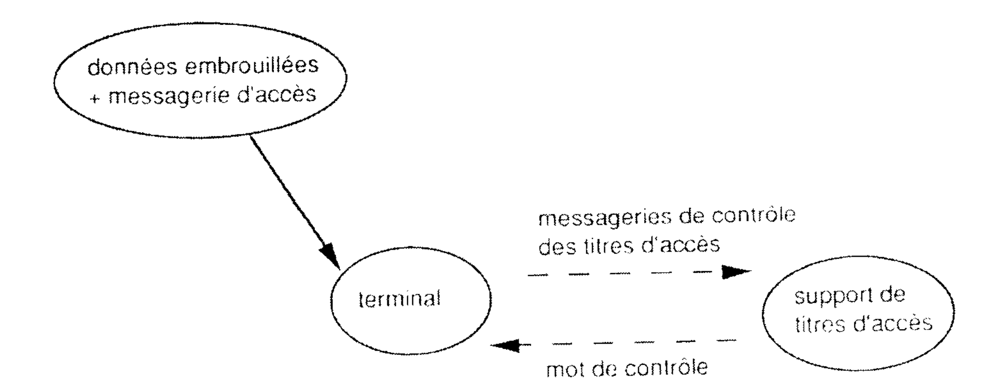
Quelques schémas permettront de mieux comprendre la mise en oeuvre de ces principes :

. L'utilisation de la messagerie de contrôle des titres d'accès :



. Les échanges d'information entre le terminal et le support de titres d'accès :

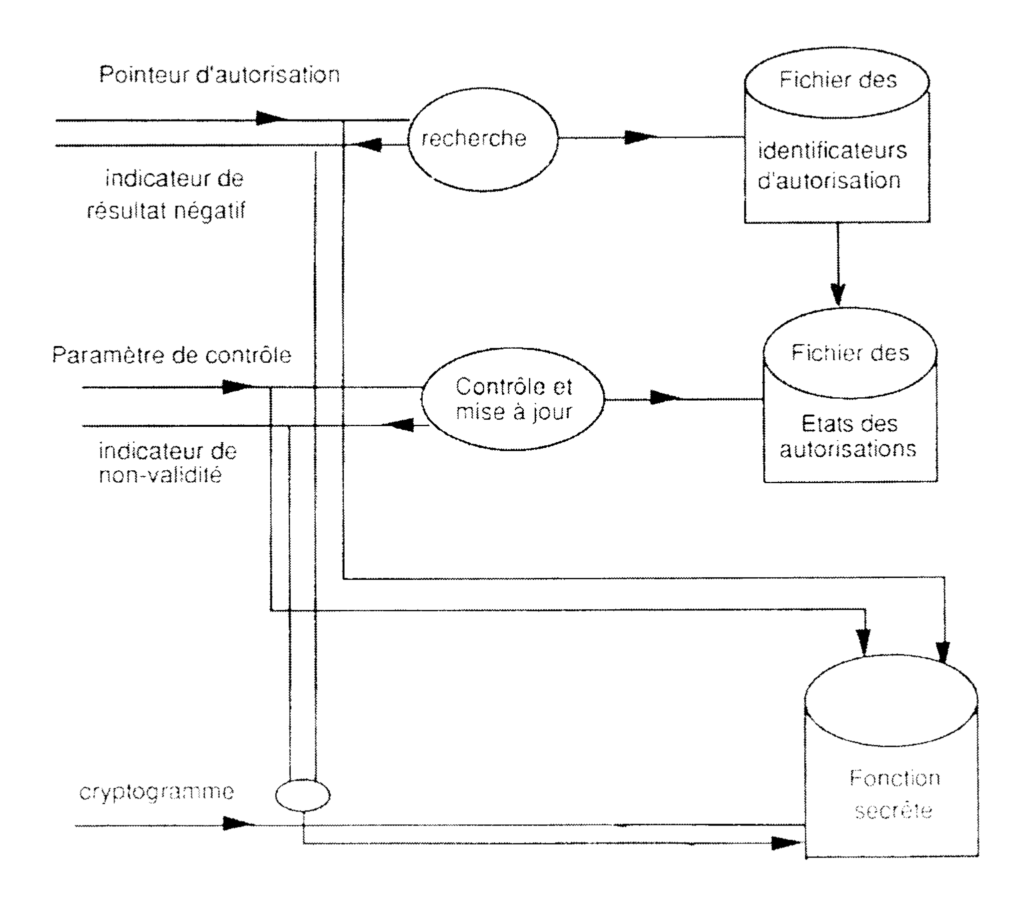
données embrouillées
+ messagerie d'accès



La correspondance entre messagerie de contrôle des titres d'accès et fonctions du support de titres d'accès (fonctions développées plus loin :)

SUPPORT	MESSAGERIE
Identificateur d'autorisation	Pointeur d'autorisation
Etat de l'autorisation	Paramètre de contrôle
Fonction secrète	Cryptogramme du mot de contrôle

. Fonctionnement schématique du support d'accès :



A la suite de son expérience du télétexte, et de son approche des services professionnels TDF a développé un service de diffusion de données transparent.

Pour ce service, comme pour le télétexte, le besoin d'un système d'accès conditionnel a été ressenti.

Celui-ci a été spécifié en 1986, il utilise des principes très voisins de ceux mis en oeuvre pour le télétexte et a donné lieu au développement d'une chaîne de diffusion complète avec en particulier les éléments suivants [3-4] :

- Embrouilleur,
- Contrôleur des titres d'accès (organe générant les messageries de contrôle des titres d'accès calculées par des cartes mères),
- Récepteur de données avec lecteur de cartes à mémoire,
- Centre de gestion des titres d'accès permettant d'introduire les autorisations dans les supports des usagers (carte à mémoire), avec en particulier la possibilité de distribution des autorisations à distance par un service vidéotex.

Un tel centre de gestion est maintenant mis en oeuvre depuis 2 ans par SDIB pour ses services CHRONOVAL et CHRONOPTION.

L'embrouillage des signaux de télévision fait classiquement appel à des processus pseudo-aléatoires synchronisés au codage et au décodage ; la mise en oeuvre de ces processus nécessite de faire appel à une diffusion de données.

Les procédés utilisés au départ de la télévision à péage en France utilisaient des Générateurs Pseudo-Aléatoires de petite taille et linéaires, et un accès conditionnel rudimentaire caractérisé par :

- Procédé par distribution du mot d'initialisation,
- Transport des messageries de contrôle d'accès par le courrier.

Un tel système se contente d'une diffusion de données à très faible rythme (1 bit par ligne de données et 1 ligne de données par trame, soit 50 eb/s).

Toutefois, diverses caractéristiques sont maintenant demandées, qui nécessitent une révision de cette conception :

. Générateur Pseudo-Aléatoire de plus grande dimension, avec structure non linéaire. Cela nécessite l'acquisition de mots de contrôle de taille croissante (couramment 64 bits, parfois plus) et oblige à la réalisation du dit Générateur Pseudo Aléatoire en logique câblée, eu égard aux vitesses de traitement nécessaires.

. Variété des modes d'accès aux émissions, avec en particulier des modes d'accès rapide :

- Abonnement à durée fixe,
- Abonnement à durée variable [par ex. abonnement "Week-end"],
- Abonnement thématique,
- Emission ou événement programmé à l'avance [pay per view],
- Emission ou événement sans choix préalable [impulse pay per view],
- Durée ou consommation.

. Nécessité de mettre en oeuvre un mode de transmission des autorisations plus sûr que la simple distribution des mots de contrôle [système à distribution d'autorisations].

. Adressabilité, c'est-à-dire émission des données d'autorisation dans le signal vidéo et non par le courrier ou un autre moyen externe au système.

Des systèmes fonctionnant suivant ces principes peuvent se contenter de transmissions de données à 8 bits/ligne, 1 ou 2 lignes de données par trame, soit 400 à 800 eb/s [3-5] mais peuvent nécessiter des débits de données beaucoup plus importants selon le parc d'abonnés à gérer et la complexité des protocoles de communication mis en oeuvre.

4. INDEXATION DES EMISSIONS ET MESSAGES ALPHA-NUMERIQUES

Si l'on désire mettre en oeuvre des modes d'accès thématique ou de type "pay per view" dans les procédés à distribution d'autorisation, alors l'identification précise des émissions devient nécessaire. Elle est habituellement obtenue par diffusion dans le signal vidéo d'un certain nombre d'Identificateurs et paramètres dont le volume détermine la finesse de segmentation des plages d'accès disponible.

La mise en oeuvre de procédés d'embrouillage assurant une opacité totale de l'image pose à l'utilisateur un problème d'identification de l'émission reçue et non décodée. C'est pourquoi il est demandé fréquemment de permettre la transmission de messages alphanumériques ou graphiques permettant cette identification par incrustation dans l'image du téléviseur. Cela va jusqu'au titre de l'émission en cours, et aux messages adressables. Les divers codes temporels (EBU, SMPTE) utilisés en production répondent partiellement à ces besoins mais nécessitent en général un support séparé du signal de télévision.

La nécessité de satisfaire ces besoins a conduit au développement des techniques qui ont abouti :

- A la voie d'identification des services dans les systèmes MAC, laquelle permet à l'usager d'identifier l'émission et d'en sélectionner les composantes,

- Aux systèmes de messageries de programmes destinés à la télécommande des magnétoscopes des usagers depuis la source des émissions.

5. CARTES A MICROCIRCUIT

L'accès conditionnel en radiodiffusion et la carte à micro-circuit sont apparus dans le panorama des techniques à peu près en même temps et, très tôt, il a paru intéressant de faire appel à la carte à micro-circuit pour réaliser un certain nombre des fonctions du système d'accès conditionnel.

Dès l'origine, on a acquis la conviction que la carte à micro-circuit présentait pour les applications d'accès conditionnel deux avantages décisifs :

. C'est un support détachable, et, en tant que tel, elle permet de banaliser le terminal de l'usager,

. C'est un support inviolable : il permet de conserver des informations secrètes tout en garantissant l'impossibilité de relire ces informations de l'extérieur.

En raison de son coût, la carte à micro-circuit n'a pas pu être introduite dans le domaine des applications grand public dès l'origine de celles-ci ; en l'occurrence, l'utilisation de la carte à micro-circuit n'a pas pu être retenue pour la première génération de terminaux de Canal Plus, mettant en oeuvre le système DISCRET.

Par contre, ces considérations de coût avaient un impact plus faible dans le cas de services professionnels et, en outre, la sécurité apportée par la carte à micro-circuit devenait un facteur déterminant.

C'est ainsi qu'a été entrepris le développement de la première carte à micro-circuit porte-clé PCO [3-2].

La carte PCO peut être considérée comme une sorte de bloc note mémorisant des autorisations ; une autorisation peut être définie comme l'ensemble des données permettant de donner l'accès à un service.

Ces données sont pour l'essentiel de 3 types :

. Un identificateur qui permet de sélectionner ou de rechercher une autorisation sur la carte,

- Des conditions d'accès : dates de validité d'un abonnement, coût d'un programme,

- Des clés secrètes qui viennent paramétrer un algorithme cryptographique et permettent de recalculer les mots de contrôle, ces clés constituant l'élément secret dont la relecture depuis l'extérieur est impossible.

L'utilisation de PCO a permis de prendre conscience de certaines limitations :

- Existence sur la carte du seul algorithme direct et donc impossibilité d'assurer la fonction carte-mère avec le même support,

- Pas de possibilité de paiement à la consommation,

ces limitations ont conduit au développement du porte-clé vidéotex dit PC1 [5-1] qui offre ces possibilités, sachant que le paiement à la consommation n'est pas un paiement à la durée.

Par contre dès PCO, le contrôle de l'inscription des titres d'accès dans la carte, et en particulier des clés secrètes, a été conçu en faisant intervenir une autorité émettrice, seule détentrice d'une clé dans la carte : c'est là la fonction de la zone émetteur de la carte inscrite dans celle-ci à sa mise en service et qui en permet le contrôle tout au long de sa vie.

Une nouvelle étape sera franchie avec le développement du porte clés PC2 qui, outre l'affinement des fonctionnalités de PC1, permettra d'introduire la notion de portage du support de titres d'accès entre opérateurs de service (tout en préservant l'indépendance de ces opérateurs).

6. LES PROTOCOLES DE COMMUNICATION DE L'ACCES CONDITIONNEL

Le développement des systèmes d'accès conditionnel aux services de radiodiffusion a conduit aux développements de protocoles de communication. Ces protocoles permettent aux opérateurs de service d'acheminer vers les cartes à micro-circuit supports de titres d'accès, d'une part les conditions d'accès aux programmes diffusés, d'autre part les autorisations à inscrire dans les cartes.

Différents systèmes de diffusion de données ont été imaginés pour diffuser l'une ou l'autre ou les deux de ces messageries, par exemple :

Système à 48 bits/ligne proposé par RPIC,
Systèmes basés sur DIDON ou UK-Teletext,
Utilisation de porteuses numériques,
Utilisation du multiplex numérique des systèmes MAC-PAQUET.

Dans tous les cas les conditions d'accès aux programmes sont diffusées avec le signal de programme lui-même ;

les autorisations peuvent être distribuées par d'autres réseaux que le réseau de diffusion (par exemple service videotex) mais l'utilisation du réseau de diffusion est particulièrement avantageuse dans le mesure où elle n'implique aucun investissement supplémentaire en moyens de communications ; tel est le but du service d'adressage sur antenne qui fournit le véhicule de distribution des autorisations.

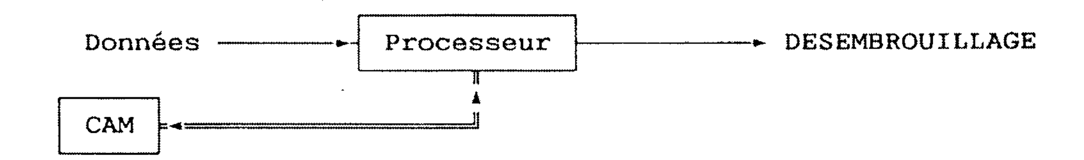
Cependant quels que soient les systèmes de diffusion de données proposés et les moyens de transport envisagés, la distinction entre les messageries véhiculant les conditions d'accès et les messageries véhiculant les autorisations s'est imposée et a conduit aux notions désormais communément admises d'ECM (Entitlement Checking Message-Messagerie de contrôle des titres d'accès) et d'EMM (Entitlement Management Message-Messagerie de gestion des titres d'accès).

Dans ce contexte, le processeur de décryptage devient un simple convertisseur de protocole entre :

. Les circuits d'acquisition de données,

. Les circuits de désembrouillage (configuration du Générateur Pseudo Aléatoire),

. La carte à microcircuit.



7. EMBROUILLAGE DU SON

Depuis les débuts de la télévision cryptée en France, le son est traité en bande de base, par retournement du spectre audio au moyen d'une modulation de type BLU effectuée après préaccentuation.

La fréquence de transposition est fixe, et son choix est discutable, résultant d'un compromis entre la qualité de la réponse voulue aux basses fréquences pour l'ensemble de la chaine et les capacités de modulation des émetteurs son en haute fréquence.

Ce compromis s'établit à 12 800 Hz (soit 256 x 50 Hz) pour les émetteurs en norme L, mais PHILIPS a également produit des matériels fonctionnant à 13 800 Hz [7-1], et des propositions ont été faites par d'autres firmes pour un retournement autour de 15 625 Hz [7-2], ce qui, il faut bien l'avouer, parait bien naturel et bien tentant...

D'autre part, afin de contourner les difficultés dues à l'insuffisance de la réponse en haute fréquence des émetteurs son de télévision et de pallier les dégradations liées à l'enregistrement du son des émissions avant décryptage, PHILIPS a récemment proposé de remplacer ce traitement de retournement de spectre par un processus de translation de spectre obtenu par une technique de double retournement [7-3] ou de double modulation BLU. Dans ce cas, la préaccentuation avant traitement devient inutile et le signal brouillé peut se manipuler aussi simplement qu'un signal non brouillé, tout en étant inintelligible.

Quoi qu'il en soit, ces procédés analogiques de traitement du son ne sont pas satisfaisants dans la mesure où ils dégradent considérablement la qualité sonore et où ils sont stationnaires, ce qui en rend le piratage très aisé.

Il faut donc faire intervenir, comme pour le cryptage de l'image, des grandeurs cryptographiques permettant une variabilité du traitement audio, et remplacer les opérations de simple "brouillage" évoquées ci-dessus par des véritables méthodes de cryptage.

Un procédé récemment proposé par PHILIPS consiste à faire varier d'une manière aléatoire, la fréquence de transposition utilisée dans un système à retournement de spectre, ou mieux, le déplacement de fréquence procuré par un système à double retournement de spectre (mode dynamique) [7-4].

D'autres procédés existent, fondés sur des manipulations temporelles de portions de signal (obtenues par mémorisation numérique) et transmission analogique [7-5].

Le point commmun à ces diverses approches, est la nature analogique de la transmission sonore, et l'utilisation du canal audio propre aux systèmes de télévision classiques, avec ses limitations qualitatives intrinsèques et incontournables.

Les méthodes les plus satisfaisantes pour obtenir un son de bonne qualité et un cryptage réellement efficace font appel à des procédés 100 % numériques (codage, traitement et transmission).

. La présence d'un Générateur Pseudo Aléatoire utilisé pour la dispersion d'énergie dans certains procédés permet aisément de crypter le son (modification du mot d'initialisation ou du GPA).

. L'indexation des émissions est en général présente dans le train numérique composite, et permet donc une gestion segmentée des autorisations.

. La présence d'une certaine capacité de données "réservée à des usages futurs" peut être mise à profit pour compléter le système d'accès conditionnel.

Lorsque le son est destiné à accompagner une image de télévision, la transmission peut s'effectuer :

. Soit dans le signal vidéo composite, sous forme multiplex en bande de base :
  - SIS [7-6]
  - D/D2MAC Paquet

. Soit sur une porteuse numérique en modulation par sauts de phase :
  - C/MAC [7-7]
  - NICAM 728 [7-8]

Dans le cas où seul le son est concerné, indépendamment de tout contexte télévisuel, on peut réaliser un accès conditionnel de même type.

Dans ce cadre général, s'insèrent les études concernant le cryptage destiné à l'anti-piratage des disques compacts audio ou des enregistrements magnétiques DAT, problèmes qui rejoignent d'une manière enore plus générale le contexte de la protection des données numériques.

8. INTERFACE HOMME/MACHINE - ERGONOMIE

Le premier système de télévision à accès conditionnel disponible dans le grand Public français a été le système de Canal + [8-1]. L'ergonomie rustique en est à la mesure de la simplicité du sytème d'accès conditionnel employé : un clavier à 10 touches permettant l'introduction manuelle d'une messagerie de contrôle d'accès de 8 chiffres (de 0 à 9), plus une touche permettant de placer le décodeur dans le mode "introduction de messagerie" et une touche de validation, ainsi que trois voyants de signalisation constituent l'interface homme-machine ... un bien grand mot !!!

L'ensemble se complète actuellement d'une manière harmonieuse par le Minitel, le serveur de Canal+ réalisant une fonction quasi-immédiate d'adressage des messageries.

Lorsqu'il s'est agi de faire évoluer les systèmes d'accès conditionnel sur la base de la même interface d'usager, la limitation principale à la flexibilité et à la sécurité du système a été d'ordre ergonomique ; cette limitation se concrétise par la sujétion créée par la nécessité de saisir et d'introduire manuellement des messageries numériques de grandes longueurs sans que cette opération ne devienne une cause d'erreurs rédhibitoires (d'autant que, pour des raisons de sécurité évidentes, il est souhaitable que le décodeur se bloque complètement après un certain nombre, assez réduit, de tentatives consécutives d'introduction de messageries erronées).

La limite a été établie avec le système RT 86 à 10 chiffres de messagerie de contrôle d'accès.

L'adressabilité directe (par envoi d'EMM sur le canal de transmission) constitue un progrès considérable en matière d'ergonomie dans la mesure où elle libère l'usager de la contrainte constituée par le pilotage manuel de son terminal. Toutefois, l'une des difficultés de l'adressabilité au plan ergonomique vient de l'aspect information de l'usager. La signalisation des droits stockés dans le désembrouilleur est en effet indispensable et se complique singulièrement pour des systèmes multi-opérateurs et multi-modes-d'accès.

On peut imaginer que l'un des premiers soucis qui ont motivé le désir précoce de mettre en oeuvre les cartes "à mémoire" dans les services à accès conditionnel était de nature ergonomique. C'est d'ailleurs, probablement l'aspect auquel le Grand Public est le plus sensible, et qui justifie

probablement le succès de la Télécarte ; Portabilité des titres (fonction "porte-clés"), fonctionnement automatique avec absence de clavier, fonction "clé parentale" assurée de facto, impression de sophistication de la technique ... etc.

Toutefois, cette approche est susceptible de rebuter certains utilsateurs et c'est pourquoi les problèmes ergonomiques se posent de manière de plus en plus cruciale avec des systèmes "sourds" (pas ou peu de commandes apparentes) et "muets" (pas ou peu de signalisations apparentes), où tout le dialogue s'effectue de manière invisible avec le microcontrôleur d'une carte à puce.

L'interface Homme/Machine la plus demandée à l'heure actuelle fait appel à :

. Télécommande infra-rouge,
. Incrustation de symboles,
. Menus déroulants, curseurs...

Elle nécessite donc un volume de logiciel important et le matériel de génération de symboles et d'incrustation sur l'image du téléviseur.

De telles interfaces Homme/Machine peuvent être simulées et développées à l'aide d'outils spécifiques [8-2].

9. ARCHITECTURE DES TERMINAUX ET DES EQUIPEMENTS D'USAGERS

L'architecture de l'installation d'usager est aujourd'hui centrée sur le téléviseur, qu'on peut décomposer en deux sous-ensembles fonctionnels :

. La partie de sélection - démodulation vidéo et son.
. L'ensemble de visualisation et de restitution du son.

L'insertion du désembrouilleur entre ces deux parties du téléviseur s'effectue naturellement par la prise "péritélévision" [2-1].

Dans un certain nombre de cas particuliers, rattachés à la télévision classique, le sélecteur démodulateur inclus dans le téléviseur ne peut pas être utilisé tel quel dans l'application de télévision à accès conditionnel, et le "décodeur" doit, tout comme le magnétoscope, être équipé d'un sélecteur démodulateur de caractéristiques adaptées :

. Réseaux câblés à plans de fréquences particuliers,
. Transmission de courte portée en micro-ondes [MMDS]
. Réception d'émissions par satellite []
. Systèmes à porteuse numérique [Nicam 728]
. Mauvais comportement de certains sélecteurs-démodulateurs vis-à-vis des signaux numériques.

Les cas des standards D/D2MAC est plus délicat à traiter.

Lorsque le sélecteur-démodulateur inclus dans le téléviseur ne peut pas recevoir le signal MAC, il devient évident que le terminal de désembrouillage doit inclure un sélecteur-démodulateur et un désembrouilleur MAC, seule la partie visualisation du téléviseur étant utilisée.

Si le téléviseur est d'origine prévu pour la réception et la visualisation d'images MAC, deux stratégies sont possibles :

. L'une des plus directes consiste à utiliser la même structure qu celle qui est connue pour les décodeurs français actuels : raccordement à la prise péritélévision. Le signal D/D2MAC crypté est prélevé sur cette prise par le désembrouilleur et restitué à la prise, soit sous forme D/D2MAC non crypté, soit, mieux, sous forme RGB décodé [].

Dans ce dernier cas, l'installation de l'usager comporte deux dispositifs de décodage de la chrominance : l'un pour le D/D2MAC, inclus dans le "décodeur", l'autre pour le PAL/SECAM, incorporé d'origine dans le téléviseur/moniteur. Le gâchis (pièces et fonctions redondantes) est évident si ce dernier est équipé d'un châssis "numérique"....

. L'autre consiste à prévoir une interface de type informatique entre le décodeur MAC inclus dans le téléviseur et un dispositif extérieur d'accès conditionnel. Le dialogue consiste à l'émission des ECM du Téléviseur vers le Sous-Système de Contrôle d'Accès (CASS) et la détermination des mots de contrôle par le Sous-Système de Contrôle d'Accès (CASS) à destination du téléviseur, ainsi que l'acquisition des EMM et leur stockage dans le Sous-Système de Contrôle d'Accès (CASS), qui inclut éventuellement la carte à microcircuit.

Cette stratégie nécessite d'importants travaux de normalisation au niveau de l'accès conditionnel, ce qui n'est pas forcément souhaitable du point de vue des opérateurs pour qui normalisation peut être synonyme de porte ouverte au piratage. Toutefois, ces travaux de normalisation progressent et un consensus semble en voie de s'établir autour de l'interface type "D2BUS" proposée initialement par Philips.

10. LES STANDARDS D2MAC

L'apparition des standards MAC (DMAC, D2MAC) [10-1] constitue en quelque sorte l'aboutissement des évolutions de la télévision au cours de la décennie ; parmi les avantages qu'apportent ces standards on peut citer :

- L'amélioration du codage de la couleur,
- Le son numérique,
- L'intégration aisée dans le standard de l'embrouillage et de l'accès conditionnel,
- La facilité d'intégration de services annexes (télétexte, diffusion de données, messsagerie de programmes, ...),
- Ergonomie d'accès aux services.

De par leur conception ces standards sont le support naturel des services à conditions d'accès. Ils permettent désormais d'envisager le développement de ces services dans les meilleures conditions techniques.

Il n'en reste pas moins que les standards MAC ont cependant leurs limitations :

- Leur diffusion hertzienne soulève encore des difficultés,
- Le standard fige le générateur pseudo-aléatoire ce qui ferme certaines possibilités d'évolution,
- Dans l'avenir, la diffusion numérique de la télévision apportera sans doute une amélioration décisive des techniques d'embrouillage.

Il est cependant rassurant de constater que le livre reste ouvert et que nous n'en avons pas écrit la dernière page.

11. CONCLUSION

En conclusion, le D/D2MAC constitue donc la synthèse d'une décennie de progrès en matière de transmission audiovisuelle : application de méthodes de multiplexage des composantes utilisées depuis quelques années dans le domaine professionnel, et ajout de fonctions complémentaires appréciables pour les opérateurs et pour les utilisateurs.

Toutefois, le D/D2MAC en clair parait bien lourd et bien coûteux pour réussir à s'imposer rapidement et se justifier facilement en tant que standard de télévision pure en remplacement du PAL et du SECAM. Son usage, en effet, nécessiterait de toutes façons une dépense supplémentaire pour le consommateur et pour le diffuseur, et ne s'appliquerait qu'au satellite et au câble.

Sa pénétration sera également liée à la qualité et l'intérêt des programmes offerts par les opérateurs. Au contraire, il se développera sans doute progressivement grâce à la valeur des services qu'il offre en plus de la télévision telle qu'on la connait actuellement :

. Le son digital multicanaux,
. Le télétexte incorporé...

et surtout, il a de fortes chances de s'imposer à moyen terme comme standard de télévision cryptée pour les grands opérateurs, du simple fait que le système est prévu d'emblée pour incorporer les fonctions nécessaires à l'accès conditionnel, qui est l'un des moyens offert aux opérateurs pour rentabiliser le lourd investissement nécessaire et l'obtention des programmes de haute qualité que ces techniques permettent - et imposent - de diffuser pour assurer leur pérennité.

12. BIBLIOGRAPHIE, REFERENCES ET NOTES

[1-1] Antiope USA.
Maîtrise d'oeuvre TDF et SOFRATEV.
Référence : CBS/CCETT "North American (NABTS) Broadcast Teletext Specification" 22/06/1981

[1-2] Document TDF : LAR/CAS/100/82/LG du 06/10/82 : "Addendum à la Spécification DIDON-ANTIOPE pour le Contrôle d'Accès"

[1-3]

[1-4]

[1-5] marché TDF n° B 9043 T notifié le 31/10/80 : intitulé : "Développement d'un dispositif de décodage TV à péage "institutionnel""

[1-6] marché TDF n° B 9047 Y notifié le 28/01/81, intitulé : "développement d'un dispositif de décodage TV crypté "grand-public""

[1-7] marché CCETT n° 86 ME 02, notifié le 16/07/87, intitulé : "étude, réalisation et fourniture d'une maquette de récepteur D2MAC/Paquet"

[1-8] marché CCETT n° 86 ME 26, notifié le 08/12/86, intitulé : "marché relatif à l'étude, la réalisation et la fourniture de maquettes de modules de contrôle d'accès pour récepteurs D2MAC/Paquet"

[1-9] Document RTIC TID-DEV/87/056/FI/LF du 17/03/87 : "Spécifications du module contrôle d'accès du récepteur D2MAC"
F. ISSALY, T. GARCIN, P. MORASSI.

[1-10] Marché France-Télécom n° 89 23 215 : "Fourniture de terminaux sélecteurs décodeurs désembrouilleurs pour service télévisuels à conditions d'accès à la norme D2MAC".

[2-1] Norme française NF C 92 250

[2-2] Brevet 76 24 304 déposé le 09/08/76 : "installation de transmission de sécurité de télévision" WESTINGHOUSE ELECTRIC CORPORATION - U S.

[2-3] procédé dit "DISCRET 3" :
Brevet Européen EP 0119 945 B1 :
"procédés et dispositifs d'embrouillage et de désembrouillage pour images de télévision "
Inventeur: C. GAUTIER
Etablissement public "Telediffusion de France"

[2-4] procédé dit "DISCRET 4"
Brevet français n° 85 101 94 :
"procédé d'embrouillage et de désembrouillage d'images de télévision"
Inventeurs: C. VICTORION, J. GUIONNET
Etablissement public : "Telediffusion de France"

[2-5] marché TDF n° B 9047 Y, déjà cité.

[2-6] Rapport final lot A (phases 1, 2, 3) du marché TDF n° B 9047 Y, daté du 29/04/1882 (J.P. ARRAGON, C. CANTOU, L.E.P.)

[2-7] marché DISCRET 11 pour CANAL + FRANCE :
- Contrat signé le 13 décembre 1983,
- Début de livraison en Juillet 1984,
- 2 500 000 décodeurs livrés à ce jour (Mars 1990).

[2-8] marché TDF n° B 9047 Y. La Radiotechnique a également mené des études dans ce domaine sur fonds propres.

[2-9] Rapport: "Application d'un couple de convertisseurs video"
M. ERNOU, S.A. La Radiotechnique, Septembre 1985.

[2-10] Brevet français n° 83 13 540 :
" G.P.A à sécurité accrue"
Inventeurs : J.P. ARRAGON, G. MARIE,
S.A. "LA RADIOTECHNIQUE".

[2-11] DISCRET 12 : premier décodeur à technologie numérique pour signaux de télévision en bande de base produit industriellement par La Radiotechnique ;
- premières livraisons en Octobre 1985 à TELECINEROMANDIE (Suisse)
- Fournitures en :
  . ISLANDE (STOD 2)
  . SUISSE (TelecineRomandie)
  . NORVEGE (OKKA TV)
  . ITALIE (RAI)

[2-12] Utilisations du décodeur DISCRET 12 (ou TDR 12) en France par l'Administration ou pour la Communication Institutionnelle :
. DTRE
. DOT (Nancy,Cergy)
. VIDEOSPACE
. PEUGEOT S.A.
. U.A.P. (voir [7-1]

[2-13] TUDI 12: premier sélecteur-désembrouilleur produit par La Radiotechnique:
- Premières livraisons en Septembre 1986,
- Utilisateurs :
. ISLANDE (STOD 2),
. SUISSE (TelecineRomandie, Telereseau),
. NORVEGE,
. IRLANDE (Cablelink),
. ANGLETERRE(British Medical TV),
. SUEDE (Televerket).

[2-14]

[2-15] Brevet français n° 88 07 781 :
"Correction d'un signal video"
Inventeur: J.P. LANDRAGIN
S.A." LA RADIOTECHNIQUE INDUSTRIELLE ET COMMERCIALE"

[3-1] Revue Radiodiffusion Télévision.
Didon-Antiope - Spécifications techniques - Norme L 1984.

[3-2] Marché TDF - C1118 Z.

[3-3] Recommandations et rapports du CCIR, 1986. Volume XI - Service de radiodiffusion (Télévision).

[3-4] Document CCETT AIS/T/05/85/DR. Didon 3 - Spécifications techniques.

[3-5] TUDI 14 : sélecteur-désembrouilleur adressable avec transmission de données à 800 eb/s, équipe :
- 2M/MAROC:
Contrat signé en Septembre 1988,
Inauguration du système complet le 03 Mars 1989,
- CANAL + BELGIQUE:
Contrat signé en Mai 1989,
Premières livraisons en Septembre 1989,
Inauguration le 27 Septembre 1989,
- L'IRLANDE (applications MMDS et câble).

[5-1] Document CCETT ASP/T/14/87/LG. La carte porte-clés PC1 - Description générale.

[7-1] Matériels fonctionnant en 13 800 Hz :
- Discret 11 modifiés pour l'UAP (communication institutionnelle, voir [2-12].

[7-2] C'était notamment le cas du système prévu par RTBF à l'intention de CANAL + BELGIQUE.

[7-3] Brevet français n° 85 05 951 :
"Système pour la transmission secrète de signaux audio et téléviseur pour la réception de tels signaux"
Inventeurs : V. CAPRARESE, Th CHRETIEN, R. DAUVILLIER,
S.A. "LA RADIOTECHNIQUE"

[7-4] Brevet français n° 87 18 045 :
"Procédé de système de brouillage/désembrouillage du son"
Inventeurs : V. CAPRARESE, D. GOGUILLON,
S.A. "La Radiotechnique Industrielle et Commerciale"

[7-5] Procédés par manipulations temporelles de portions de signal sonore préalablement mises en mémoire numériquement :

[7-6] SIS (Sound-In-Sync) :

[7-7] C/MAC :

[7-8] NICAM 728 : en réponse à la demande d'un grand opérateur pour disposer d'un son de qualité numérique sur une émission de télévision conventionnelle cryptée, PHILIPS-RPIC avait fait la proposition d'utiliser le NICAM 728, avec transmission des ECM dans les zones de données disponibles du train numérique du NICAM, et possibilité d'adressabilité à grand débit dans les cas de transmission monophonique ou d'utilisation de la voie sonore analogique seule.

[7-9] Cela est le cas de la Radiodiffusion numérique sur satellite. PHILIPS-RPIC avait notamment proposé, en réponse à une consultation de l'Administration Française, d'adapter le système proposé en Allemagne par le BMFT et l'IRT à l'utilisation sur réseaux câblés en y adjoignant un système d'accès conditionnel.

[8-1] Contrat signé le 13 Décembre 1983 ...

[8-2] Outils de simulation et de développement pour études d'ergonomie des interfaces homme-machines évoluées.

[10-1] Doc. Tech. UER 3258.
Spécifications des systèmes de la famille MAC-PAQUET.

ELEMENTS OF THE MAC/PACKET FAMILY

David **WOOD**, Edgar **WILSON**
EBU Technical Department
Case Postale 67
Ancienne Route 17A
1218 GRAND SACONNEX - GE
SUISSE
Tél : +41 22 798 77 66

Elements of the MAC/packet family

David Wood and Edgar Wilson
EBU Technical Department
Geneva, Switzerland

INTRODUCTION

The MAC/packet family of systems is the result of collaborative work by European broadcasters and manufacturers. The development began in 1981. This paper is a brief introduction to the system. It is not a detailed technical treaties. The EBU-published specification and other publications are readily available. The story is one of the most important and interesting in broadcasting technology, and the system is still in the process of expansion.

SATELLITE BROADCASTING

In the 1970s, it became clear that satellite broadcasting, **DBS**, was a practical possibility, and Europeans were anxious to plan satellite broadcasting bands so that services could begin. The existing television bands (the terrestrial services) were virtually full up. For the new age of satellite broadcasting, recourse had to be made to the higher and as-yet unused 12 GHz band.

In 1977, a worldwide conference was convened to plan the 12 GHz satellite broadcasting band, for all parts of the world except the Americas.

In Europe, it seemed likely that satellite broadcasting would use the television systems PAL and SECAM then in use. An elaborate plan was devised, whereby the 12GHz band was divided up into sets of 5 television channels, which were given to essentially all countries, large or small.

Although, just after 1977, it seemed that the PAL and SECAM vision systems were to be used for DBS, there was considerable support for using digital sound with satellite broadcasting. Both in Europe and Japan, studies were made on ways to accompany conventional television with digital sound. These reached similar conclusions, and subsequently in Japan (in 1984), a satellite was launched using the digital sound system, together with NTSC vision. This is still in use in Japan today. Essentially, the

existing sound sub-carrier for television, which is arranged to be just above the vision signal, is replaced by a package of up to four, very high quality, multiplexed digital audio signals. As explained later, this is termed an A-type system.

In Europe, by the early eighties, there was a feeling that ,while digital sound alone was a worthwhile improvement, we could also go even further, and develop an entirely new sound and vision system, The new system could bring the benefits of the new CCIR production standard, Rec 601, to the home, by using separate Y, U, V components, rather than the PAL and SECAM systems. This would provide for higher picture quality, as screens of larger size became popular.

New systems were entirely admissible in the 12 GHz broadcast bands, provided they were compatible with the interference requirements of the WARC 1977 plan.

CONVENTIONAL TELEVISION

Colour television signals, as normally broadcast, are formed by simultaneously transmitting the Luminance and Colour-difference signals. A monochrome receiver uses just the Luminance signal, to display a monochrome picture. The colour receiver uses all three to display a colour picture by re-forming the three colour Primary signals.

Because of the properties of the eye, the amount of detail present in the Colour-difference signals, U and V, need only be about one third of that present in the Luminance signals Y. This can be used to advantage in the broadcast system.

Transmitting the three signals at the same time will inevitably cause some mutual interference, but it is possible to reduce it to a point where it can barely be seen, and this is what is done in the PAL, NTSC, and SECAM systems.

The television picture is made up of horizontal lines, and the effect this has, is that the frequency spectrum of the vision signal falls in a series of bunches, rather than in a continuous spectrum. In between the bunches there are spaces, and the colour-difference information, which also falls in bunches, is arranged to fall in these spaces. The spectra are like combs. They are arranged so that the teeth of one fits between the teeth of the other.

When they are broadcast, the Colour-difference signals are moved to the part of the Luminance signal which carries fine detail. This makes them less conspicuous, and this, combined with the previous fact that only a limited amount of colour difference information is needed, makes it possible to transmit all three signals at the same time, without major interference between the components.

There are three colour television systems in operation in the world: PAL, SECAM, and NTSC. The basic philosophy of the three systems is the same. It is the simultaneous transmission of Y,U, and V signals. There are, however, slight differences in the way the U, and V are carried in each of the three systems, so receivers designed for one system cannot unfortunately decode the others.

Up until the end of the 1970s, not only television broadcasts used the PAL/SECAM/NTSC formats. The same format was used for recording and picture processing in the television studio.

At that time, the EBU proposed that there should be a new format for the production of television programmes, for which the components Y, U, and V were recorded and processed separately. The motivation for this was the hope that all Europe (or even the world) could move to the same unique production standard. It was also believed that it would lead to a higher technical quality final product.

It was also suggested that, apart from providing a source for PAL/SECAM/NTSC broadcasts, the new production source could also be a spring-board to the development of a new broadcast format, which would provide a higher technical quality service than the current colour television broadcasts.

MAC, THE NEW TELEVISION SYSTEM

In the early 1980s, it was clear that there was a growing demand in Europe for ever larger screen televisions. It did seem however that there would be limits to what would be possible, because of the bulkiness of the CRT display, and the physical size of European living rooms. At that time it seemed, in short, that a new television system which could deliver the new component standard, Rec. 601 signals to the home (but no more) was what was needed for the foreseeable future in Europe. There was enough detail to saturate the eye, for the screen sizes likely to be available. Only at a later time would it be necessary to move to 'high definition television'.

It was with this in mind that the MAC vision coding system was developed in the early 1980s. It was essentially a means of transporting to the European home, the benefit of the new studio standard, Rec 601.

In addition it seemed also important that the new system should be flexible and open-ended, so that it could be enhanced if new display systems were available to warrant it. Therefore it was intended to be extendible upwards in quality at a later date.

The MAC vision system uses a technique of time compression to transmit the Y,U, and V signals separately. Each television line of Y, U, and V is compressed in time, so there remains space in the real television line for more than one component. This idea was not new, even in 1981 when the idea was first put forward by the UK IBA. It was however only then that large scale integration made possible the practical implementation of such a system in the home receiver.

Before transmission, the television line is converted to a digital version by sampling and coding. The signal is read into a digital store at a given rate, then read out at a faster rate. On each line are included compressed versions of the luminance component and one of the two colour-difference components. In this way, the three components are transmitted separately.

When colour television was introduced, account had to be taken of the existing monochrome receivers in peoples homes. As television services evolve further, this same requirement exists. The requirement for simultaneous reception on earlier generations ,or simpler, receivers is termed **backwards compatibility**.

To achieve this in a terrestrial television service would mean that the new service has to be fundamentally based on the existing system. To achieve backwards compatibility for satellite broadcasting, there are extra degrees of freedom. This is because the viewer inevitably needs a new satellite receiver, whatever the broadcast system used. Therefore, into this receiver can be included circuitry to convert the signal to the earlier standard. The critical question in the case of satellite broadcasting is how much extra it costs to do the conversion.

The route taken with MAC was to define a system that could either be directly fed to the receiver or very cheaply converted to the old formats (PAL and SECAM). This is achieved by scanning system compatibility. The same number of lines per picture is used and the same picture rate. Conversion in the satellite receiver to PAL or SECAM costs very little, but many viewers can connect directly to the receiver, via the RGB video connector in the receiver.

In addition, the MAC system is made to suit the environment of satellite broadcasting, better than PAL and SECAM does. Satellites have particular features which makes the PAL and SECAM systems less suitable than they are for terrestrial broadcasting.

In brief, this is because in terrestrial broadcasting, the position of the colour-difference information with respect to the Luminance information does not influence how the signals are effected by noise. In satellite broadcasting the effect of noise is worse in the part of the Luminance which contains high detail. This is the triangular noise which is associated with frequency modulation, used for satellites.

In PAL, SECAM, and NTSC the high detail area is the area where the colour information is located. So, we might expect that if we used PAL or SECAM for satellite broadcasting, there would be more noise in the colour signals than in the luminance signal. This is what happens. The effect is tolerable, and it is definitely possible to broadcast PAL and SECAM by satellite , but there is a tendency for highly colored pictures to be noisy. This lack of noise is another of the benefits of the MAC system. The MAC system is designed to avoid this, because the colour information is not moved to the area of high detail as it is in PAL and SECAM.

There was another benefit of the MAC system, which some viewed as the most important of all. This was the cultural benefit of having a unique satellite broadcast standard throughout Europe. A single receiver could be used throughout the continent. This was certainly a noble idea.

As it turns out, the interests of Europe as a whole prove not to have the highest priority for the individual states.

THE MAC/PACKET FAMILY

The MAC/packet system is by no means only new in respect of its image system. In fact in the receiver, the changes in vision circuity are largely overshadowed by the changes to the sound and data circuitry. There are very important sound, data, and control aspects to the system.

The sound quality perceived by the listener depends on the capability of the broadcast system and, as always, the capability of the receiver that the viewer has. The broadcast system sets a limit to what the viewer can hear, but below this, what he actually hears is set by his home installation.

The human psycho-physical system is considered to be able to benefit from audio bandwidths of up to about 15kHz. The threshold of perception can be beyond this, but the higher frequencies do not seem to contribute to audio quality.

At the time the MAC/packet system was developed it seemed forward-looking to design a digital sound system to permit 15kHz audio bandwidth, with in-audible background noise. The system needed to allow stereo sound, or a range of alternative sound channels. These might be used for carrying alternative language versions of the television sound, or even for other independent sound services.

The system allows a number of sound coding and FEC options. All the systems are based on the use of 32 kHz sampling-frequency. The audio coding can be 14-10 NICAM or 14 bit linear.

Teletext is also an important broadcast medium, and it is feasible that other data based broadcast services will be developed in the years ahead.

The need was therefore perceived in 1982 to transport digital data for sound or other services, and to allow for extensions of the image systems at a future time. This led to the conclusion, which was quite revolutionary at the time the system was developed, that what was needed was a flexible multiplex, which could be used for a variety of services.

The broadcast signal should not only contain the services themselves, but an explanation of what was being broadcast. This could be interpreted by the receiver, which could, in turn, configure itself to the transmission. In short the system was conceived to work with an intelligent receiver. The old world, where a there was always a one-to-one relationship between the service and the channel, would be superseded, by the new world of microprocessor and flexibility.

To accomplish the above, a **service identification system** was developed, for transmission along with the picture, sound, and data. This labels and describes each component on the service, so that the receiver can adapt itself accordingly.

The original system developed was termed the **C-MAC/packet** system. The term 'C' describes the multiplex method used. The term 'packet' is associated with the fact that the sound and data signals are arranged in fixed length packets.

It may be interesting to note that this package had a pan-European origin. The **MAC** vision system was originally developed in the UK by the IBA. The **Packet** system was developed in France and the **C** system in Scandinavia. In addition a particularly ingenious part of the sound and data packet structure was devised by German engineers.

However, in the year that followed the initial development, some of the optimism for the C-MAC/packet system began to fade. Manufactures in France and Germany argued that if they were to produce receivers quickly, in time for services in 1985 and 1986, they needed to implement a simplified version of the system proposed, which had less options. less flexibility, and would allow less complex circuitry in the receiver.

Manufacturers also argued that, however well the system was tailored to satellite broadcasting, it was not well suited to local re-transmission on some cable networks.

For all these reasons, France and Germany drew up their own variant of the system, termed the **D2-MAC/packet** system. This offered a limited range of options for the sound and data signals, and half the sound and data capacity of the original C-MAC/packet system.

Later in the 1980s, again at the suggestion of receiver manufacturers,a further system was developed, which retained the original features of the C-MAC/packet, but allowed a slightly simpler home receiver. This was the **D-MAC/packet** system. This effectively superseded the C-MAC/packet system.

The D2-MAC/packet and D-MAC/packet systems are considered to be (founder) members of the **MAC/packet family.**

For the two members of the family many elements are the same. This includes the methods of vision and sound coding. However, the data capacity of the D2 system is half that of the D system. The D multiplex is effectively two D2 multiplexes side-by-side.

The EBU hoped that manufacturers would market receivers which received both and accepted both systems. This unfortunately is not happening for commercial reasons, although there have been some more positive developments on this matter recently.

The EBU's original classification for DBS systems is as follows:

A SYSTEMS

Frequency multiplexing, with a picture signal, of a digitaly modulated sound and data sub-carrier

B SYSTEMS

Baseband time multiplexing, with the picture signal, of a full response digitally coded sound and data signal

C SYSTEMS

Radio frequency time multiplexing of a sound and data system with the picture signal

D SYSTEMS

Baseband time multiplex of a picture and a sound and data system with partial response coding (more specifically duo-binary coding)

CONDITIONAL ACCESS

Every television service provider needs the means to finance the programme production. Satellite services require initial funds to pay for the satellite launch and subsequent running costs. Equally, programmes which draw large audiences are often expensive to produce. One means to make this equation work is pay-television, or **Conditional Access**. Technically such systems have two parts.

The first is the process of rendering the picture, and possibly also the sound, unintelligible unless special measures are taken. This is termed the **Scrambling** system.

The second is the mechanism for conveying the information to the viewer on how to make the picture coherent. This is known as the **Encryption** system.

There is normally a conflict in picture scrambling systems, in that the scrambling systems which are the most secure can also leave the most residual picture impairments when they are de-scrambled. This is slightly less of a problem with the MAC vision system, because of the compression process used.

The Encryption system can take a variety of forms, however some of them require large amounts of data capacity to be available ('Over-air addressing'). This is no problem for the MAC/packet system, which is designed for data transport. Thus on balance, the MAC/packet system is particularly well suited to Pay-TV, because it is less susceptible to impairments, and also can cope with any kind of Encryption system.

It proved relatively easy to agree on a universal Scrambling system for the MAC packet family, but this was not the case for an Encryption system. Some broadcasters saw the use of an individual Encryption system as a commercial advantage, and would not agree to a unique European system. Their logic was that if the user has a specific system, just for your channel, he is less disposed to use (and thus watch) someone else's channel. Having invested, he would be something of a captive market.

Time will tell if this was a short sighted perspective.

The general principles of the conditional access system are as follows. The different components (picture, sound, data) are first scrambled by a pseudo-random binary sequence(PRBS) from the scrambling sequence generator. The start point in the cycle of the PRBS generator is defined by a so-called "control word".

There may be a "local" control word (a fixed binary word) built into the receiver which can be used where there is to be free access to the programme. The receiver can descramble the signal without other decryption data. Where access is to be controlled or not free, a variable control word can be encrypted by a two tier "authorization key". This in turn is encrypted by a "distribution key". To decrypt the encrypted authorisation key, the user uses his personal distribution key, together with the encrypted authorization key (the Entitlement Management Message or EMM), which may be transmitted with the broadcast signal, or sent by some other physical means. To obtain the control word, the user needs the authorization key and the encrypted version of the control word. The signal can then be descrambled by a pseudo-random binary sequence identical to that used for scrambling.

The entitlement checking message and the entitlement management message (respectively, the encrypted version of the control word and the encrypted authorization key) can be both transmitted in the packet multiplex, or the EMM can be conveyed to the subscriber by other means (e.g. post), depending on the type of key management system (the " access control system")

The MAC vision scrambling is done by cutting and rotating active picture line segments. It is possible to define, by a pseudo random binary sequence, either a cut point in the luminance and in the colour difference (the double-cut component rotation process) or a single cut point in the colour difference signal (the single cut line rotation process). The first process offers higher security but is somewhat more sensitive to line tilt distortion, and amplitude-frequency response distortion which can occur in cable networks or the RF stages of receivers. The overall response required for line tilt is about 1% to 5%, depending on the masking effect of any noise in the picture.

The digital signal is scrambled by modulo-2 addition of a pseudo random binary number.

DEVELOPMENTS IN THE MAC/PACKET FAMILY

The MAC/packet family is not static, and the specification is now being further developed in two major areas.

FULL-CHANNEL MODE

The first is the so called **full-channel mode**. In this mode, the channel is totally given over to the carriage of data signals, or sound and data signals. Thus it is possible to broadcast information services for education or other industries and services. The

DBS channel has a relatively large capacity for doing this, and where there are large numbers of users all wanting the same data it makes good economic sense to use this system.

The second development is to a high-definition television member of the MAC/packet family.

HDMAC

In 1986 an European development programme, Eureka 95, was initiated with the objective of developing technology for all parts of an HDTV broadcasting chain. This involved a large number of European manufacturers, broadcasters, and Universities. The plan was to increase the level of know-how in Europe about HDTV. HDTV was seen as a vitally important emerging technology, which might affect a numbers of industrial sectors. Research in Japan had already reached an advanced stage, and there seemed a risk of Europe being left behind.

The project developed an HDTV member of the MAC/packet family, which is termed **HDMAC**. This system has exactly the same sound and data arrangement as the lower members of the MAC/packet family. The difference is solely in the potential picture quality. There are currently, strictly speaking two variants of this system: **D/HDMAC** and **D2/HDMAC**. It remains to be seen if only can be finally chosen for universal use.

The concept of 'high-definition' quality is a relatively difficult one to pin down. It was originally defined , at the EBU suggestion, to be a quality such that a high definition picture would be indistinguishable from a window on the real world. In other words, the eye would be saturated with detail, to the extent that there was no point in increasing it.

Moving from the general concept, to numbers which could be interpreted in electrical terms, is not straightforward. Firstly, the detail that the eye needs to saturate it, depends on the brightness of the display, and other display factors. Second, as mentioned above, it depends heavily on the distance between the viewer and the screen, and the content of the scene. From very close to the screen, it needs a lot of definition. From further back, assuming the screen size remains the same, relatively little detail is needed.

To design an HDTV system, therefore, we have to make some assumption about the size of the screen and where the viewer is sitting. When we have this information, we can choose electrical parameters to suit. Work done in Japan suggests that about the largest-sized screen people could readily accept in their homes will about one square meter. Their work also showed that the preferred viewing distance varies with the

type of programmes. When there is a lot of movement in the picture, people prefer to be further back. Where there is not, they prefer to move forward. On average, however, a viewing distance of three times picture height seemed to be a good bet for the circumstance where the screen is at least one square meter in size. From this assumption we can calculate ,broadly, the amount of detail required to saturate the eye.

When studying how to up-grade the performance of the MAC system to a high-definition version, it transpired that by doubling the number of lines per picture and the horizontal resolution, the requirements of a domestic high definition service, as mentioned above, can be met.

In a broad analogy, the picture quality of the HDTV picture might be seen as similar to 35mm film. Thus, in the broadcast environment, we could see PAL, MAC and HDMAC as equating broadly with Super 8mm film, 16 mm film, and 35mm film. As with the film standards, how good the pictures are in each case, depends on the screen size. Each provides good quality pictures on progressively larger screens. In the television environment therefore, these three standards would mirror the progressive increase in home television screen size.

The design problem for HDMAC was therefore to develop such a system which would fit into the channel width offered by the satellite broadcasting bands. This had to be done while maintaining compatibility with the existing MAC signals. Existing receivers should still be able to receive a picture when the high definition signal is being broadcast.

The proposed HDMAC system is based on extending the time period over which the picture is built up. The system is arranged such that, when the picture is stationary, it is built up over a period which is twice as long as used for conventional television. When the contents of the picture are moving, the picture is built up over the conventional period. What is more, the picture is split up into a very large number of blocks, each of which can use the longer build period, if the contents warrant it. The longer build-up allows the receiver to assemble a more detailed version of the block.

The above is a considerable simplification of a very sophisticated system. There is no formal full specification available, at the time this document is being written,

The picture quality available to the viewer was not yet evaluated at the time this paper is being written. The EBU hopes to perform formal subjective assessments on the system in the second half of 1990.

The critical issues will be whether the changes in the picture build-up time leaves visible impairments in the picture. This will show in how the system behaves with critical moving pictures. It will also be important to evaluate the picture quality of the

picture when received on conventional MAC receiver, to see if the fact that an HDTV picture is actually being broadcast leads to impairments.

CONCLUSIONS

The development of the MAC packet family is a considerable technical achievement. It showed that Europeans can work together, even if there are signs that national considerations take precedence when there is a clash of interests.

ACKNOWLEDGEMENTS

The MAC/packet system was developed by a large number of engineers from many different laboroatories. It would be impossible to mention all their names here. Nevertheless, they have the satisfaction of knowing the contribution they made, and they have the great appreciation of the EBU Technical Commitee.

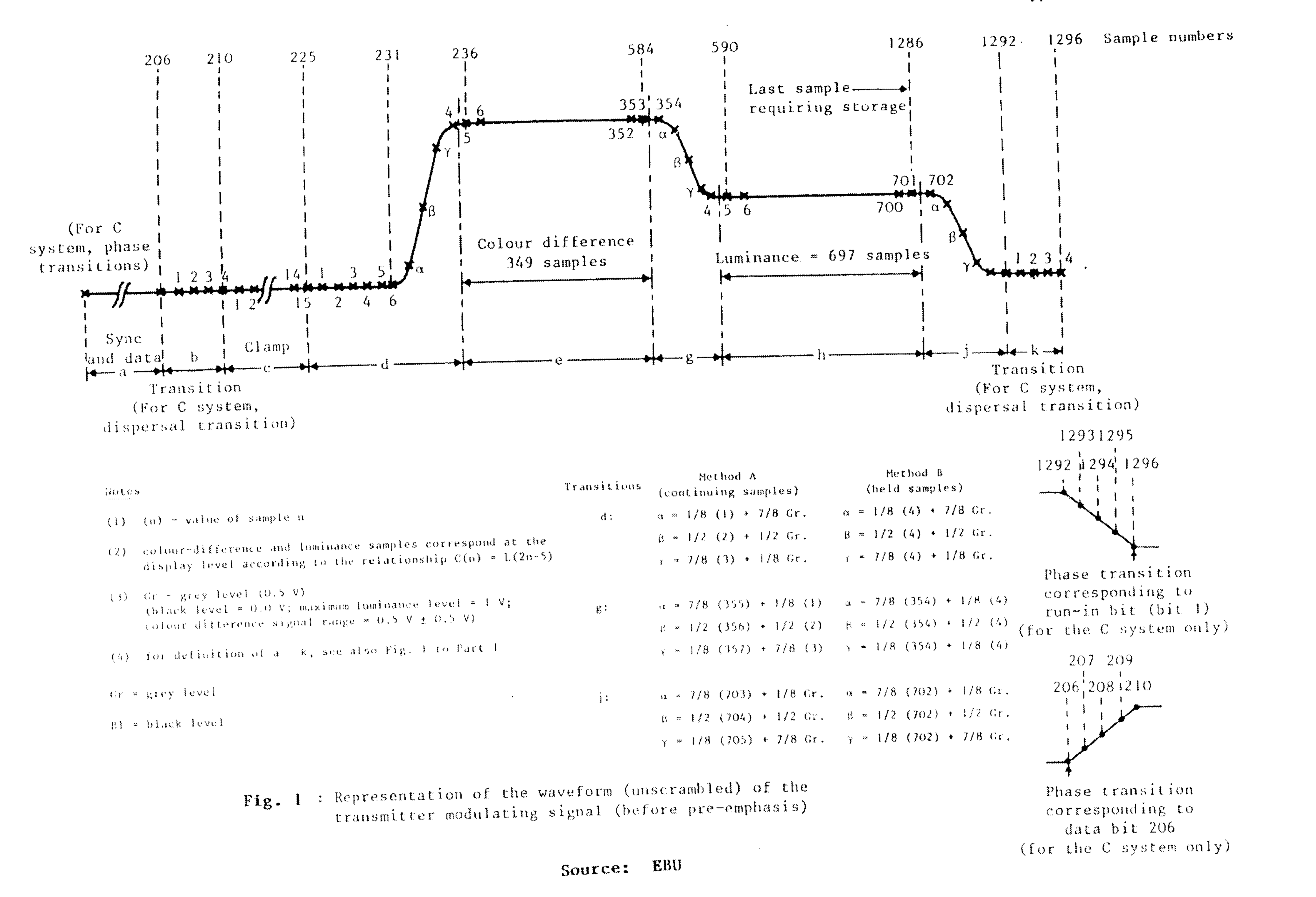
REFERENCES

1. The C-MAC/packet system for direct satellite television
   Mertens. H. and Wood. D.
   EBU Review-Technical No 200 (August 1983)

2. Specification of the systems of the MAC/packet family
   Tech. 3258 E (English) and Tech. 3258 F (French)
   EBU Technical Centre, Brussels, Belgium, October 1986

3. Specification du systeme D2-MAC/pacquets
   (English translation, for international use, from the original french)
   Telediffusion de France, September 1985

DW
May 1990



Notes

(1) (n) = value of sample n

(2) colour-difference and luminance samples correspond at the display level according to the relationship C(n) = L(2n-5)

(3) Gr = grey level (0.5 V)
(black level = 0.0 V; maximum luminance level = 1 V;
colour difference signal range = 0.5 V ± 0.5 V)

(4) for definition of a – k, see also Fig. 1 to Part 1

Gr = grey level

Bl = black level

Transitions	Method A (continuing samples)	Method B (held samples)
d:	α = 1/8 (1) + 7/8 Gr.	α = 1/8 (4) + 7/8 Gr.
	β = 1/2 (2) + 1/2 Gr.	β = 1/2 (4) + 1/2 Gr.
	γ = 7/8 (3) + 1/8 Gr.	γ = 7/8 (4) + 1/8 Gr.
g:	α = 7/8 (355) + 1/8 (1)	α = 7/8 (354) + 1/8 (4)
	β = 1/2 (356) + 1/2 (2)	β = 1/2 (354) + 1/2 (4)
	γ = 1/8 (357) + 7/8 (3)	γ = 1/8 (354) + 1/8 (4)
j:	α = 7/8 (703) + 1/8 Gr.	α = 7/8 (702) + 1/8 Gr.
	β = 1/2 (704) + 1/2 Gr.	β = 1/2 (702) + 1/2 Gr.
	γ = 1/8 (705) + 7/8 Gr.	γ = 1/8 (702) + 7/8 Gr.

Fig. 1 : Representation of the waveform (unscrambled) of the transmitter modulating signal (before pre-emphasis)

Source: EBU

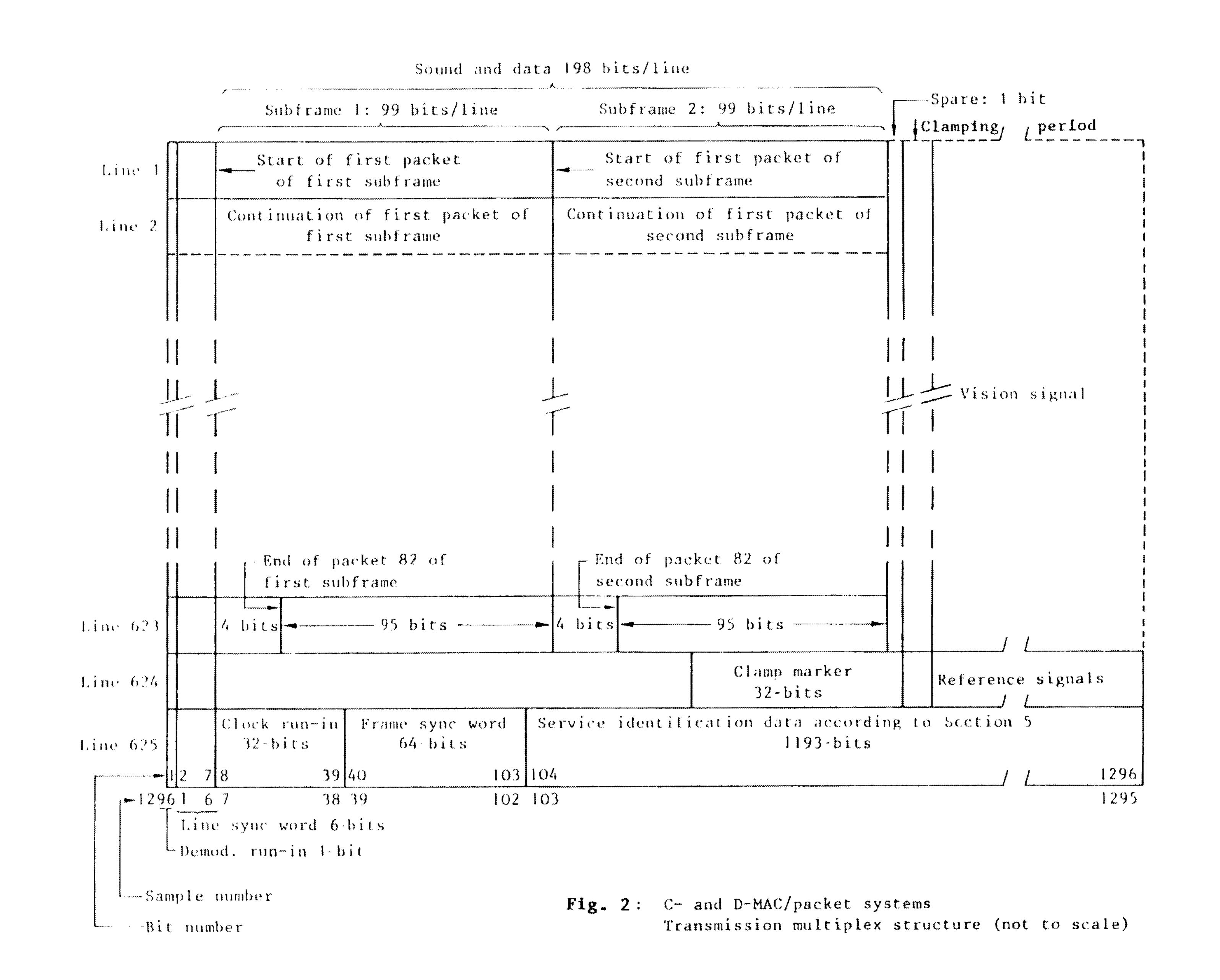
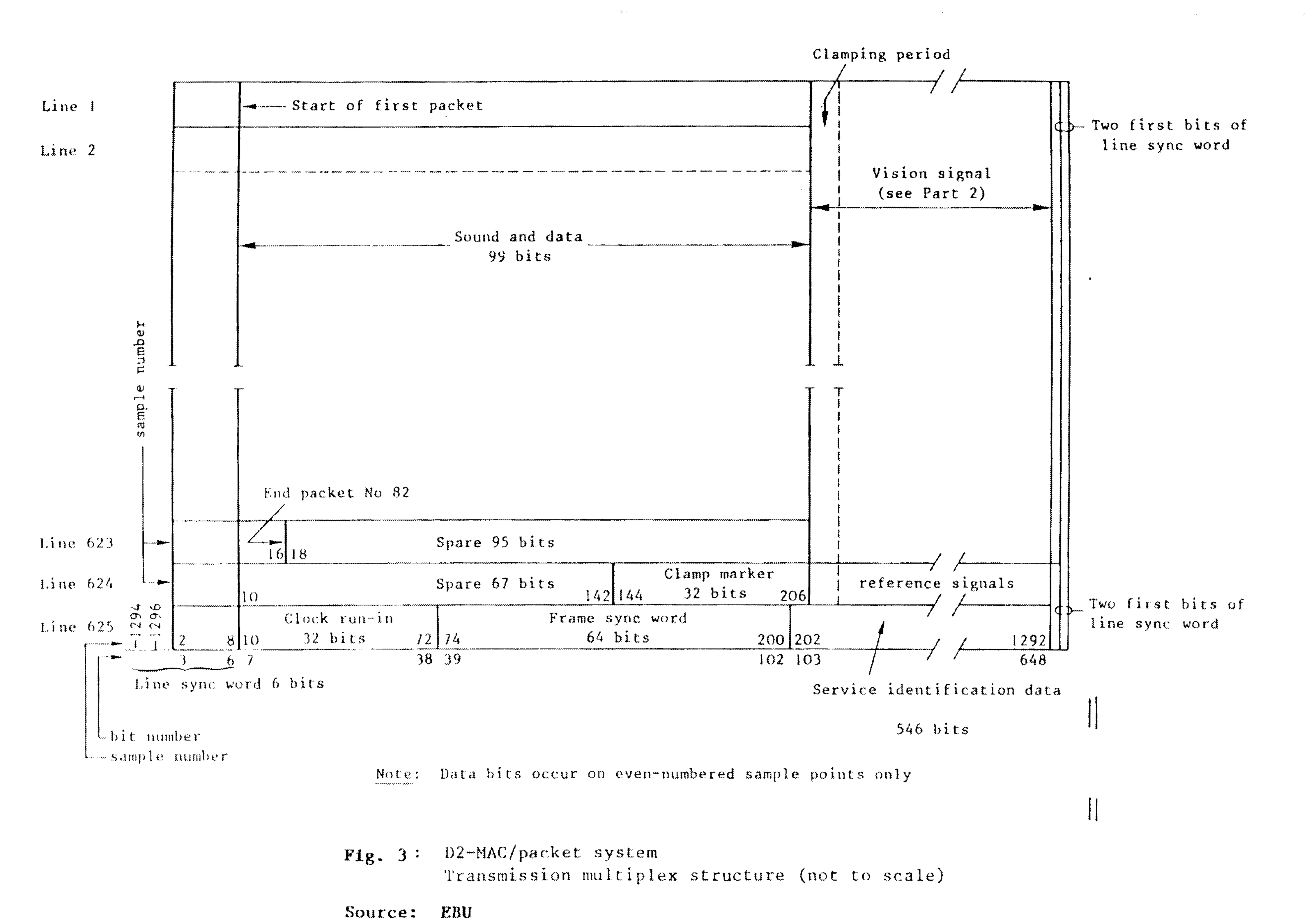


Fig. 2: C- and D-MAC/packet systems
Transmission multiplex structure (not to scale)



Note: Data bits occur on even-numbered sample points only

Fig. 3: D2-MAC/packet system
Transmission multiplex structure (not to scale)

Source: EBU

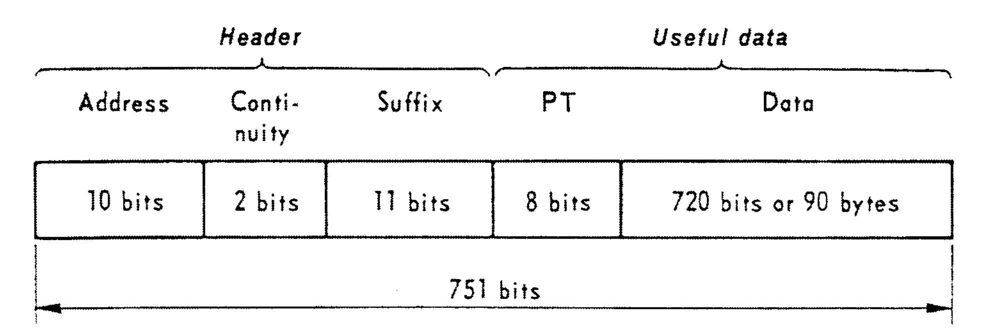
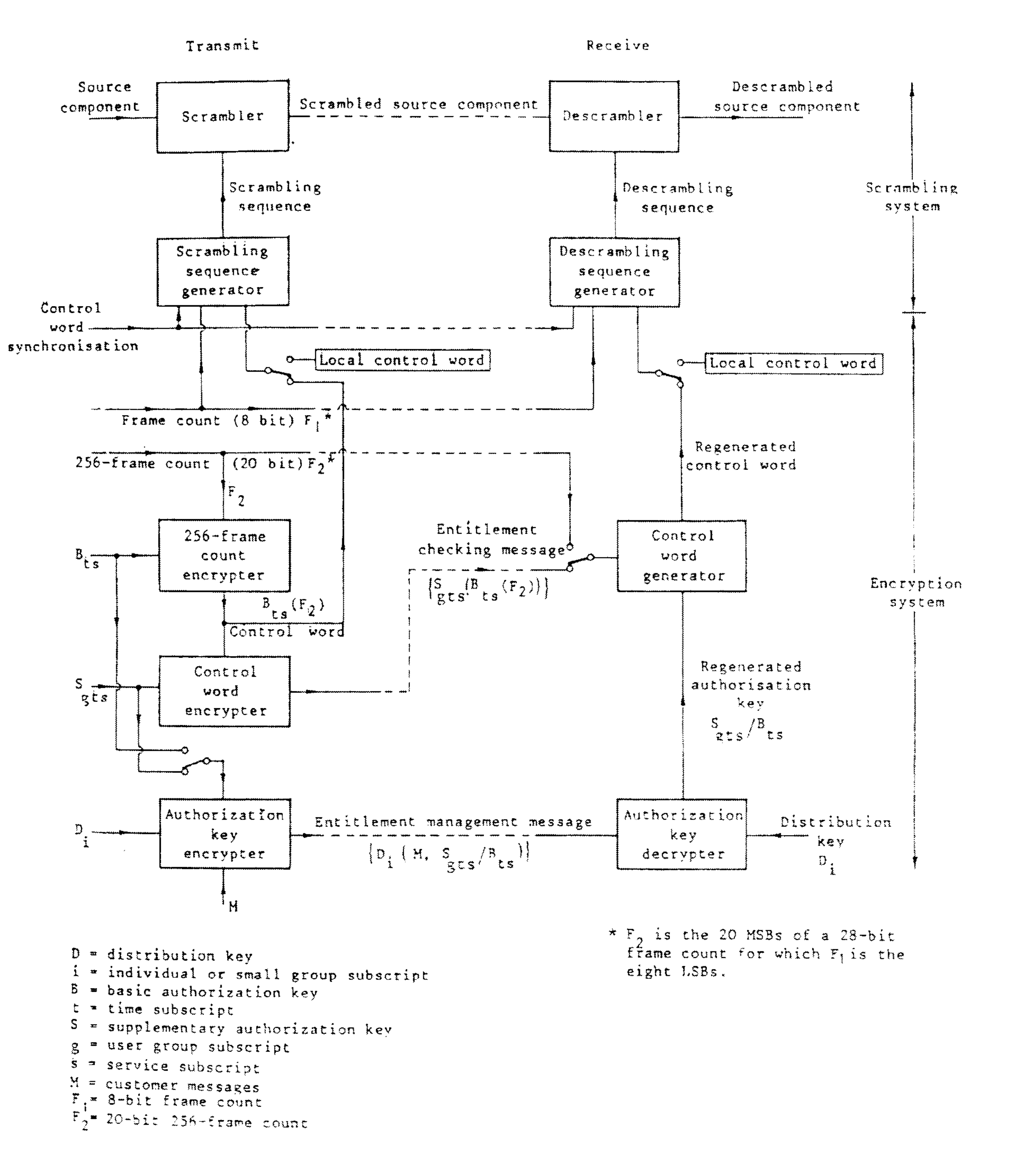


Fig. 4 : Packet structure

Fig. 4

Source: EBU



D = distribution key
i = individual or small group subscript
B = basic authorization key
t = time subscript
S = supplementary authorization key
g = user group subscript
s = service subscript
M = customer messages
F_1 = 8-bit frame count
F_2 = 20-bit 256-frame count

* F_2 is the 20 MSBs of a 28-bit frame count for which F_1 is the eight LSBs.

Fig. 5 : Generalised block diagram of the conditional access system

Source: EBU

THE ARCHITECTURE AND SECURITY DESIGN GOALS OF THE EUROCYPHER SYSTEM

Chris **BENNETT**, Paul **MORONEY**
VideoCipher Division
General Instrument
6262 Lusk Bvld
SAN DIEGO, CA 92121
ETATS UNIS
Tél : +1 619 455 1500

David **CUTTS**
European Television Encryption Ltd
Welby House
96 Wilton road
LONDON SW1V 1DW
ROYAUME UNI
Tél : +44 71 233 6388

TABLE OF CONTENTS

THE ARCHITECTURE AND SECURITY DESIGN GOALS OF THE EUROCYPHER SYSTEM

Chris Bennett and Paul Moroney, VideoCipher Division of General Instrument,

David Cutts, European Television Encryption Ltd

1 BACKGROUND

This paper outlines the architecture of the Eurocypher conditional access system. Eurocypher is an enhancement of the VideoCipher II system, which has been used since January 1986 to provide signal security to cable programmers transmitting in C-band in the United States and Canada. The VideoCipher Division (VCD), then part of M/A-COM Inc, began actively promoting the use of a VideoCipher-based system for European DBS and cable broadcasting in July 1986, initially for PAL-based systems and then for MAC systems. In May 1988, a contract was signed between General Instrument, who had acquired VCD in the meantime, and British Satellite Broadcasting Ltd (BSB) to develop an implementation of Eurocypher access control for BSB's DBS services in the United Kingdom, and suitable for use by other programmers. Eurocypher has been in operation for BSB since March 1990, and is proposed as a standard for conditional access in MAC systems to the European Broadcasting Union (EBU).

The Eurocypher system design is intended to allow implementations which will support the conditional access requirements of any MAC programmer. It is designed to meet the requirements of the MAC standard [EBU86] of the EBU, which has been adopted by CCIR and is required for use in DBS broadcast satellite television within the European Community [EEC86].

The system is an integral part of the total satellite television system supporting the programmers' communications. The objective of the system design is to supply the following characteristics:

- High security for the transmission of satellite television signals, based on highly secure access control procedures.

- Flexible tier control capable of supporting a wide variety of operator requirements.

- Consumer access to any programmer using Eurocypher through a single piece of equipment.

- Independent access control for simultaneous transmission of MAC-delivered services cable and certain SMATV headends as well as directly to Direct-To-Home (DTH) households.

- Independent access control for simultaneous transmission of different types of MAC-delivered service (TV, radio, data etc) to different target markets and receiver types, and the ability to access two independent services simultaneously on the same channel.

- Flexible addressing and authorisation control for many millions of DTH

subscribers and commercial units.

- Simple procedures for providing rapid access and reliable authorisation updates for consumers subscribing to many channels.

- Ability to interface to D-MAC or D2-MAC signal format, depending on the requirements of individual programmers.

- A large selection of ancillary features, including programme naming, personal message service, parental lock-out, fingerprinting, impulse pay-per-view, regional and circular blackout, diagnostic screens, and replacement of active video by tier-addressed messages or teletext.

The Eurocypher system design differs from VideoCipher II in the following major respects:

- VideoCipher II signal scrambling and encryption is eliminated; MAC techniques are used instead. Eurocypher only provides conditional access. Accordingly, the Eurocypher equipment in the receiver consists of an Access Control Module (ACM), which does not include the signal descrambling inherent in VideoCipher II descramblers.

- System security incorporates many upgrades resulting from techniques developed to protect VideoCipher against active piracy attacks seen in the United States.

- System authorisation capacity is enhanced from 56 tiers per category to 512, to take advantage of the multiplexed service capacity provided by the MAC signal format.

- System message protocols are adapted to conform to the requirements of the MAC specification.

- System features are extensively adapted to the more complex requirements of the European environment.

2 SYSTEM COMPONENTS

The major system components of the Eurocypher system as implemented for BSB are illustrated in Figure 1.

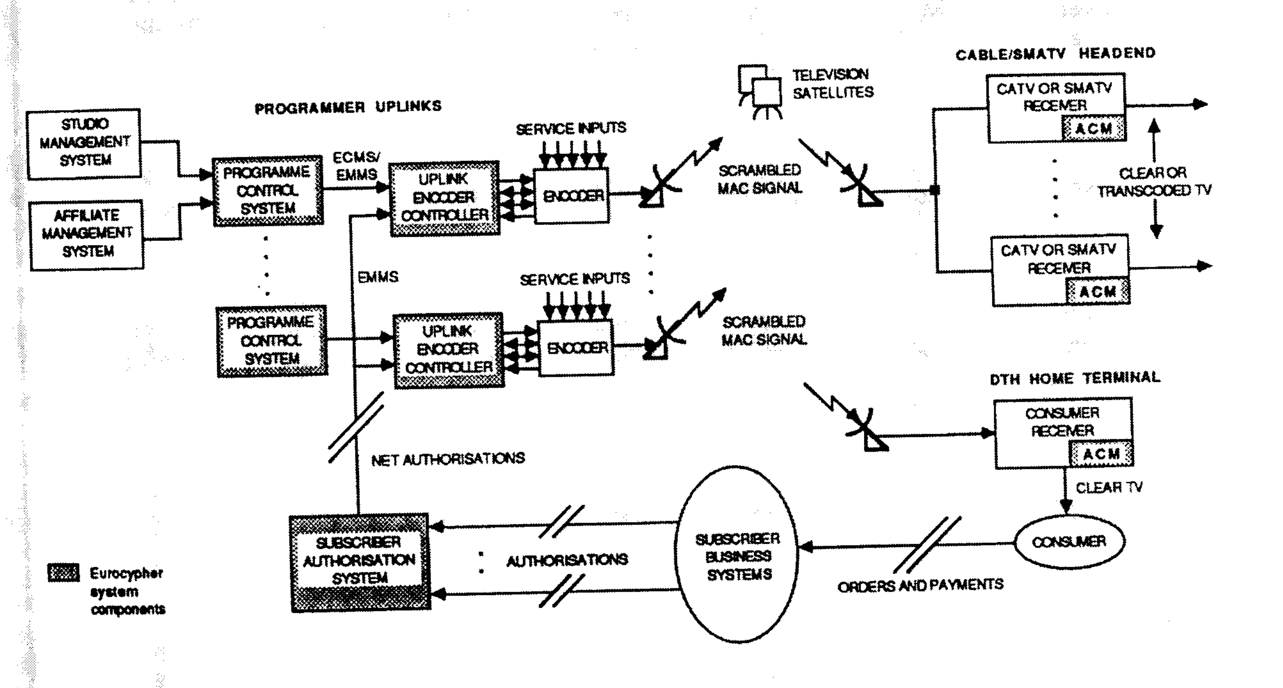

PROGRAMMER UPLINKS
STUDIO MANAGEMENT SYSTEM
AFFILIATE MANAGEMENT SYSTEM
PROGRAMME CONTROL SYSTEM
ECMS/ EMMS
UPLINK ENCODER CONTROLLER
SERVICE INPUTS
ENCODER
EMMS
PROGRAMME CONTROL SYSTEM
UPLINK ENCODER CONTROLLER
SERVICE INPUTS
ENCODER
TELEVISION SATELLITES
SCRAMBLED MAC SIGNAL
SCRAMBLED MAC SIGNAL
CABLE/SMATV HEADEND
CATV OR SMATV RECEIVER
ACM
CLEAR OR TRANSCODED TV
CATV OR SMATV RECEIVER
ACM
DTH HOME TERMINAL
CONSUMER RECEIVER
ACM
CLEAR TV
CONSUMER
NET AUTHORISATIONS
SUBSCRIBER AUTHORISATION SYSTEM
AUTHORISATIONS
SUBSCRIBER BUSINESS SYSTEMS
ORDERS AND PAYMENTS
Eurocypher system components

Figure 1

2.1 Access Control Module

Access control of the receiver is implemented by an Access Control Module (ACM), which can be a buried or detachable receiver component interfacing to the receiver circuitry which processes and descrambles the MAC waveform. The ACM implemented for BSB is a buried module, which also incorporates extensive text display capabilities.

The ACM may be incorporated into receivers at cable or SMATV headends, or into receivers which are in consumer homes. Cable and SMATV systems require a separate receiver and ACM for each channel descrambled at the headend, while consumers require a single receiver and ACM capable of accessing any or all services for which the user wishes to gain access. In addition, commercial services, such as MAC-delivered data services, will require a receiver with an ACM dedicated to the commercial service.

The ACM is a separate module with a fixed defined interface. Any receiver architecture conforming to this interface and capable of acquiring the appropriate authorisation messages can incorporate an ACM. One possible architecture is shown in figure 2. In this architecture, the ACM interfaces with a microprocessor performing the MAC SI functions, which in turn interfaces directly with the MAC decoding and descrambling circuitry as embodied in one of several vendor chip sets. This interface supports commands and control messages to the ACM, and responses and control words from the ACM. The ACM can be configured to pass data through to an external detachable ACM instead of processing the data itself.

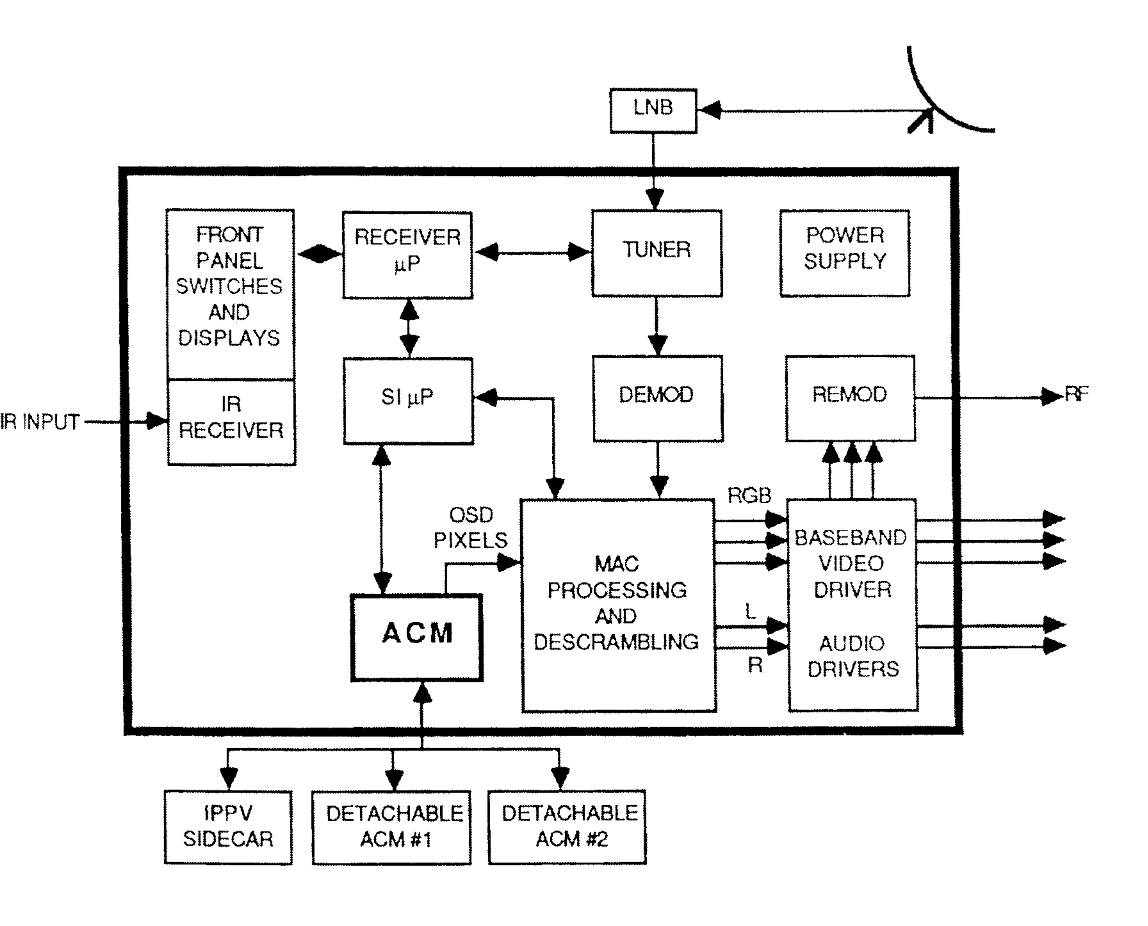

LNB
FRONT PANEL SWITCHES AND DISPLAYS
RECEIVER µP
TUNER
POWER SUPPLY
IR INPUT
IR RECEIVER
SI µP
DEMOD
REMOD
RF
OSD PIXELS
MAC PROCESSING AND DESCRAMBLING
RGB
BASEBAND VIDEO DRIVER
L
R
AUDIO DRIVERS
ACM
IPPV SIDECAR
DETACHABLE ACM #1
DETACHABLE ACM #2

Figure 2

The basic functions of the ACM are to provide:

- access control for the service selected by the consumer.
- MAC control words for initiating descrambling of the service
- user interface support for features such as parental rating (described in more detail below)
- text display capabilities for the receiver

The ACM can provide access control for two services simultaneously.

2.2 Uplink System Components

The Eurocypher uplink system equipment includes:

Programme Control System (PCS), responsible for defining the access requirements for various services, scheduling television programming, and maintaining and distributing authorisations for ACMs which are dedicated to the channel controlled by the PCS. Typical examples of ACMs which are authorised by the PCS are ACMs associated with commercial affiliates of the programmer, or ACMs providing access to commercial services such as data. Service access control requirements can be provided to the PCS over an external DECNET interface by a Studio Management System (SMS), which also control the playout of the programmer's material. Authorisation for PCS-controlled ACMs can be provided over the same interface by an Affiliate Management System (AMS).

Subscriber Authorisation System (SAS), responsible for maintaining and distributing authorisations for ACMs associated with consumer receivers. The SAS accepts authorisations over an X.25 interface from one or more business systems, which are used by retailers who sell programming packages to the public. The SAS determines the net authorisation of the ACM, and distributes that authorisation to the ACM over all channels using Eurocypher access control.

Uplink Encoder Controller (UEC), interfacing the PCS and SAS to the MAC encoders. The UEC also generates the MAC control words needed to initialise the scrambling of MAC video and encryption of MAC digital audio and data. The UEC developed for BSB is designed to interface to the encoder developed by Tandberg Telecom [Stephansen90].

The PCS and SAS are implemented on DEC VAX computers - the PCS in a rack-mounted uVAX II, and the SAS in a 6210. For different population sizes, different VAX configurations would be used to implement the SAS; upgrades will occur from time to time as the subscriber population grows. The PCS and UEC are configured in a spared configuration to allow for uplink redundancy with fast switchover. The SAS is configured as a VAX cluster with volume shadowing.

With additional enhancements, described in [Bagenal90], the system can support distributed SAS architectures for authorisation of ACMs for programmers with multi-national services. With additional enhancements, also described in [Bagenal90], the system can support collection of Impulse Pay-Per-View (IPPV) reportback data and audience survey data, and distribution of this data to business systems supporting IPPV programmers.

As implemented, the Eurocypher system uses over-air addressing techniques to maintain and update ACM authorisations. While smart-card delivery could be implemented if required, over-air techniques were chosen for consumer convenience as well as for the ease, speed and cost effectiveness of updates provided to the programmer. The advantages of over-air delivery become particularly apparent when considering the operation of IPPV systems.

A central aspect of the system architecture, which is unique to VideoCipher systems such as Eurocypher, is the coordination of DTH ACM authorisations by the SAS, and the distribution of authorisation messages created by the SAS for DTH ACMs across all Eurocypher channels. At each of the programmer uplinks, the SAS authorisation stream is combined with the channel-specific PCS authorisation stream and inserted into the MAC waveform by the UEC for broadcast to the ACMs. Since each transponder thereby contains DTH messages for all Eurocypher channels, a DTH customer receives the authorisations intended for his ACM no matter which Eurocypher channel is being watched. This simple structure removes the need for many architectural complexities which arise in over-air addressing systems based on maintaining separately acquired authorisation records in the ACM for each programmer or programmer group.

The Eurocypher approach to distribution of ACM authorisations is only feasible if the interests of the programmers are protected. Commercially, the SAS is placed under the control of an organisation such as European Satellite Services Ltd, which is open to the participation of all interested programmers. Technically, protection is provided by separating the business system and SAS functions. The SAS does not maintain any commercial data related to the users of the ACMs: this is maintained on the business systems which interface to the SAS. Thus, the integrity of each programmer's commercial data is assured by the privacy of the arrangements made between the programmers and the business system operators. Each business system provides the SAS with only the identity of an ACM and the set of services for which that ACM is authorised by the business system. The SAS prevents a business system from authorising ACMs for services without the agreement of the programmer providing the services, and strictly protects the confidential nature of the minimal data it receives from the programmers.

3 SYSTEM FEATURES

3.1 Service Authorisation

The fundamental feature offered by the system is access control to individual services through tiering. A tier may be thought of as a switch in an ACM which, if turned on, authorises the ACM to access some service associated with the switch. Each ACM receives an individually addressed authenticated message over the air which defines the set of tiers that the ACM is authorised to permit the receiver to access. For each service in the system, the PCS controlling the service broadcasts an authenticated statement of which tier is needed to access the service. If the ACM is authorised for the required tier, the receiver is permitted to access the service, either directly, or through impulse purchase.

Each ACM in the system can be authorised for any tier within a group of 512 tiers. Up to 256 different tier groups can be defined within the Eurocypher system design. The set of ACMs which can access a particular set of 512 tiers is called a category. The

assignment of meaning to the individual tiers is determined by the operators of the uplink computers associated with the management of the categories to which the tiers belong. In practice, a single tier in each category is typically used to control the ability of ACMs in that category to access a given service, or it may define a level of privilege within a service (basic or premium). Tiers associated with different categories can be assigned the same meaning, in order to allow ACMs in separate categories to be authorised to access the same services.

The system is currently implemented to support a separate category for each MAC channel, and a system-wide category for ACMs in DTH receivers across all MAC channels. The programmer would normally use the channel category to authorise ACMs integrated with commercial receivers, such as CATV receivers or receivers dedicated to commercial data services. This category is controlled by the programmer's PCS. With suitable upgrades to the PCS, additional categories can be supplied for an individual channel if the 512 tiers supplied with the normal configuration prove insufficient.

The system-wide category defines the access rights for all ACMs supporting DTH receivers. This category is controlled through the SAS. The DTH category represents an agreement by participating programmers to allow consumers the right to purchase the services of any of these programmers. The definition of the tiers within the DTH category is agreed by all participating programmers. As described above, the authorisation messages for the category are distributed across all channels supporting the category. This approach allows the ACM in the consumer's receiver to receive authorisation updates for up to 512 tiers with a single message, regardless of which channel the consumer is tuned to.

With the category approach to authorisation and tiering, the programmers participating in a category retain complete control of their commercial customers through their commercial categories, complete control over the authorisation of consumers for access to their services by ensuring that only their business systems can access their tiers, and complete control over the security of their services through provision of a level of keying in the PCS which is inaccessible to the SAS.

The business systems of the individual programmers are responsible for authorising the consumers for individual tiers. The Eurocypher system is designed so that authorisation to descramble a set of services may be sold as a package, which would represent the access right to a set of programming represented by one or more tiers. The system design puts no technical limitation on who is allowed to sell packages to the public or on the programming content of the packages. Different packages sold by the same or different retailers are allowed to contain the same tiers.

3.2 Advance Pay-Per-View

The tier mechanism can support Advance Pay-Per-View (APPV), with certain restrictions. In this mode, a tier is associated with a specific programme and a consumer who has ordered the programme before it is shown is authorised for that tier. On completion of the programme, the consumer is deauthorised for the tier.

APPV is a mode of system operation which can require a supporting infrastructure far in excess of that required for normal consumer authorisation service. In addition to the additional MAC control channel bandwidth which may be required, full support for

call-ahead pay-per-view requires the availability of much more powerful SAS and business system computers capable of processing much higher volumes of consumer transactions. Additionally, large numbers of telephones and telephone operators (or automated answer devices) are required to support the volumes of consumer traffic which may be generated. Typically, these resources would only be fully utilised very occasionally, for major events.

For these reasons, APPV is seen as an interim system to be used until Impulse Pay-Per-View (IPPV) has been installed, or as an adjunct to IPPV.

3.3 Impulse Pay-Per-View

The DTH subscription system is capable of supporting IPPV, with certain upgrades, consisting of the distribution of an appropriate reportback capability, and the addition of an appropriate control and data collection facility - the IPPV Management System (IMS). The ACM provides the control features required for IPPV. It authorises and authenticates the purchase, collects the view history data and reports it to an external unit via a serial interface provided by the receiver. The external unit reports the view history data back to an IMS, which validates the data and disburses it to the business systems entitled to receive it. The external unit can be configured so that reporting will only occur when there is data of interest to report, and the time of reporting can be configured so that the load on the telephone system and IMS is maintained at a fairly constant level, and so that reporting costs are minimised.

With the IPPV enhancements, the system allows the programmer to offer the consumer individual programmes on an impulse basis. If the consumer has established an account for IPPV with the programmer's business system, the consumer is enabled for a tier defined to allow IPPV access, and is able to order available offerings through the ACM user interface. Screens that describe current or future programme offerings are provided to the consumer. These screens are specified by means of control messages from the PCS, which will allow the ACM to display the programme's name and the price in the local unit of currency. The displayed price for a given program can be different in different countries, if required. Consumer access to IPPV is password-protected. The programmer can allow the consumer to view a portion of the programme without purchase, as a free preview, and can also prevent the consumer from buying the programme after a certain time.

To provide secure control over the consumer's rate of expenditure, a single "credit limit" register is provided in the ACM. This allows a total virtual credit limit to be downloaded to the unit from the SAS. This is checked against a "debit register" which contains the accumulated sum of programme "costs" over the lifetime of the ACM. The ACM does not allow the consumer to spend beyond the limit set by the difference between the debit and credit registers. The consumer is only permitted to access the credit for a programmer if the ACM is authorised for the programmer's IPPV tier.

The relationship between the "credit limit" register in the ACM and the consumer's actual account is determined by the business systems. The IMS maintains a small credit float, set by the business systems, which is typically related to the maximum amount of unaccounted expenditure the programmers are willing to tolerate. The relationship between this float and the consumer's actual credit limit is managed by the business systems on the basis of the view history information returned through the IMS. As the IMS receives authenticated view history data, the ACM "credit" is updated to maintain

the consumer's float, based on the "cost" of reported data. This data is returned to the business systems, so that the programmer knows the total amount of actual outstanding debt. If the consumer exceeds the true credit limit held in the business system for a particular programmer, the business system can deauthorise the ACM for the programmer's IPPV tier.

3.4 Audience Survey

The same reportback mechanism used to collect IPPV data, when available, can also be used to survey the viewing habits of an audience of non-purchaseable programming. An ACM can be tagged, through the SAS, as a participant in an audience survey. Programmes of interest to the surveyor are tagged through the PCS, and participating ACMs will record these programmes in a separate view history stack. From time to time, the participating ACMs will report the audience survey data to a collection site.

3.5 Regional Blackout

The system provides the programmer with a number of capabilities which modify the basic access control provided through tiering. The first of these is regional blackout. An ACM is assigned a region code by a programmer's business system via a control message from the SAS. Region codes are defined system-wide, and an ACM may be assigned at most one region code at a time. It typically refers to a national entity, such as France, but may refer to actual regions, such as Scotland or Bavaria, if appropriate. 64 region codes are supported, which is expected to be sufficient to cover the major separate legislative regions of the European area.

When a PCS is configured for a set of services, the set of regions which the programmer using the PCS can access is limited to the programmer's franchise area. As part of the description of the access requirements for each service, the programmer defines the set of regions within his franchise area which are permitted to access the service. An ACM which is not in a permitted region will not provide service access, even if the ACM possesses the tier required for the service. Regional blackouts are normally associated with a television programme. The same mechanism can be used to define a regional blackout for a shorter period of time, for example to black out advertisements within a programme.

3.6 Circular Blackout

The system also supports local blackouts of television programmes. The location of the receiver, identified by the subscriber's post-code or telephone number, is downloaded to the SAS at installation time by the programmer's business system. The SAS maintains location translation tables which translate from the source location data to a three-dimensional Cartesian co-ordinate, which is then loaded into the ACM by the SAS. These location tables are provided for each country as part of the process of installing Eurocypher service within that country. Each SAS will maintain a location table for each country served by that SAS. Each PCS will maintain a similar location table for each country served by the programmer operating the PCS.

To black out a local region, a command is sent by the programmer via the PCS which defines a blackout circle. The programmer specifies a location code and a radius, which is translated internally into a Cartesian co-ordinate and a radius. This defines an approximately circular region whose exact boundaries correspond to the post-code or

telephone regions whose centres are included in the circle. Each ACM determines if it is in the specified blackout region. If it is, it denies access to the associated programme. Up to 32 such circular regions may be associated with any programme, each of which can have a radius of up to 512 miles (820 km).

3.7 Parental Lockout Control

The ACM provides the means for the consumer to set a parental lockout threshold for the receiver. If a programme has a higher parental lockout rating than the threshold selected by the consumer, then access to the programme is denied by the ACM, unless the consumer enters a correct password.

The consumer is also required to provide a password before the ACM allows the parental lockout threshold to be altered. The consumer is allowed to change this password, but only by providing the valid password before requesting the change. The system provides a capability in the SAS to reset the password to a default value if the consumer forgets his password. Two types of ratings are provided. The first type of ratings are based on standard film censorship classifications for different countries. Since rating standards vary from country to country, a PCS supporting a multinational programmer would allow the programmer to define a rating level for each individual region. The ACM supports a text table which allows it to display a rating level according to the standard alphanumeric codes of its region. This table is broadcast by the SAS, and may be changed from time to time as rating codes are defined or deleted.

The second type of ratings classifies the programmes by content. The programmer can indicate that a programme contains sexual or violent material,or bad language, to allow parental lockout based on programme content. This type of rating is applicable to all countries. Both types of rating can apply to the same programme.

3.8 Text Features

Since a high proportion of television sets in the United Kingdom do not support SCART interfaces, it was determined that teletext was not a suitable medium for text display in the first generation of BSB receivers. The ACM provides support for menu-driven on-screen displays for the receiver in a 16 by 31 character format, through interaction with the On-Screen Display (OSD) circuitry included in the ACM.

The ACM OSD supports upper and lower case white characters, with blue, black or transparent background and shadowing or blocking of characters on a line by line basis. Lines may contain normal or double size characters, and characters may be underlined or blinking. The character set implemented for BSB supports English, together with additional graphics characters for use in creating boxed messages. The character set is defined to be upgradable to support all European languages using Latin-based scripts, through the addition of other characters and overlay circuitry to support accents and diacritical marks.

This facility provides the user with access to a number of local capabilities, including the ability to set or change passwords, and to set or override ratings thresholds. A diagnostic screen is provided, which allows an installer or repairman to diagnose the state of the ACM. The ACM will also display the name of the current or next programme, and at the programmer's option will display the time remaining in the current programme. The programme name will be incorporated into IPPV order

screens and view history screens. The programmer can specify whether the name of the programme is to be displayed to ACMs which are not authorised to receive it.

Using the ACM text facility, it is possible to send a personal message from the SAS to individual ACMs for display by the OSD chip in the ACM. A personal message is limited in length to one screen. Display of the message can be forced, or it can be stored for later viewing. A "message arrival" indicator signals the presence of a stored message which has not yet been read. It is also possible to send "tier-addressed" messages to all ACMs viewing a channel which fall into specified classes of access control. These messages are sent from the PCS for display by the OSD chip in the ACM. As with personal messages, display may be queued. Display may also be constrained to lie within a time window, or be of indefinite duration. The ACM can be instructed to include its address as part of the display, to assist in fingerprinting tapes which infringe copyright.

A wide variety of filters can be specified to determine the set of ACMs which may display a tier-addressed message:

- ACMs which do or do not possess a specified tier.
- ACMs which are in a specified set of regions.
- ACMs which are or are not subject to circular blackout.
- ACMs which are or are not authorised.
- ACMs which do or do not possess valid keys
- Any combination of the above.

Using the same filtering techniques, it is possible to specify generalised service replacement definitions. It is possible to include a teletext overwrite command in the tier-addressed message, identifying a teletext service and specifying a teletext page within the service to be acquired. It is also possible to specify a replacement audio service, or to identify a substitute MAC service of any kind, which need not even be on the same channel. These facilities provide a means for advertisers and/or programmers to replace television advertisements or blacked out programmes with tier-addressed or teletext messages, or with substitute services.

The ACM OSD can also be used by other components of the receiver as a display device. Typical uses include additional user menus and signal level displays.A captioning facility has also been proposed within the MAC specifications which would allow the receiver to use the OSD to display subtitles in various languages, or captions for the deaf.

4 CONTROL SIGNAL STRUCTURE

4.1 Control Signal Format

The Eurocypher control channel is a set of packet streams within the MAC sound/data multiplex. The ACM authorisation stream is identified within the MAC Service Identification (SI) channel as an "over-air addressing" service. The authorisation messages are sent as Golay (24, 12) encoded Entitlement Management Messages (EMMs), as required by the EBU MAC specifications. EMMs may be up to four packets in length. The authorisation data is sent as unit-addressed messages. A shared-address option exists for updating security data in ACMs which do not change

authorisation state, although this is not implemented at this time. Some ancillary data, such as national ratings tables, are sent as broadcast EMMs at a low frequency. Most EMMs are generated by the SAS, but some are also supplied by the PCS; the UEC is responsible for multiplexing EMMs.

Authorisations could alternatively be supplied by non-broadcast means such as memory cards or telephone dial up if appropriate. Use of alternate means can substantially reduce the net bandwidth requirements for the authorisation channel. However, such means remove the operator's ability to provide realtime response to changes in situations where rapid update is required, such as credit updates for IPPV systems. They also increase the cost of operating the system. For these reasons, over-air addressing is recommended.

Service-related control data is sent as Golay (24, 12) encoded Entitlement Checking Messages (ECMs) from the PCS, in packet streams whose addresses are identified within the SI channel. An ECM stream may define the access control requirements for certain components within a service, for all components of a service, or for a number of services. The association between the packet address of an ECM stream and the service components, service or services protected by the ECMs are identified within the SI channel. ECMs defining fundamental access requirements are sent as category-addressed messages. Ancillary ECMs, e.g. definitions of program attributes such as program names, or tier-addressed messages, are sent as broadcast messages.

4.2 Bandwidth Requirements

The bandwidth needed to support ECM streams for individual services depends on the complexity of the access requirements for the service and on the desired acquisition time for a subscriber tuning to the service. For most services, the bandwidth allocation is typically 2 ECMs per second. For a television service accessed by several categories with a complex set of local blackouts, multinational ratings and supporting tier-addressed messages, where a total acquisition time of 1 second or less is required, the informational bandwidth needed for ECMs may be as high as 9 kbps.

The bandwidth required to support the Eurocypher over-air addressing service is a function of many factors: the size of population being supported, the stability of the authorisation state of that population ("churn"), the rate at which keys delivered in the EMM stream change, the bit error rate of the channel, and the percentage of time that the population of receivers can be assumed to be listening to the channel ("coverage"). The rate of change of keys delivered in the EMM stream is fixed to be approximately monthly, and for a subscription service in steady state, the churn rate can be assumed to be fairly low. Thus, the two dominant variables are the size of population and the degree of coverage.

The Eurocypher system design was based on the requirement that Eurocypher should be able to grow to support a satellite television industry which could, in time, become pan-European in scope. In such a system, the population is likely to become large, but quite high levels of coverage can be assumed, through the distribution of SAS output across all Eurocypher channels and the use of channel homing techniques that are activated when the receiver is placed in standby mode. On this basis, and assuming optimally efficient forms of unit-addressed messaging, it was calculated that a total control channel information bandwidth of 120 kbps was sufficient to support up to 100 million ACMs under suitable operating conditions. A control channel which used the

capacity of a 15 kHz compounded audio channel with level 1 error protection - 180 kbps before Golay encoding - could then support up to 150 million ACMs. With 100 kbps of the 120 kbps control channel bandwidth assigned for ACM authorisation traffic, the system design is capable of delivering key changes for up to 1 million ACMs every hour using unit-addressed messages (720 million authorisation messages a month). The actual maximum addressing rate will be somewhat lower, due to overhead arising from changes in authorisation for some ACMs and other factors. In the current system, certain practical limitations also exist, in that the SAS injects traffic into the system at 64 kbps, and does not yet fully optimise the message formats.

The amount of bandwidth required to support changes in authorisation will depend on the dynamics of consumer behaviour. The operator of the SAS can dynamically adjust the percentage of control channel bandwidth allocated to supporting authorisation changes. While the system is in a state of growth, a larger proportion of the channel would be allocated to this purpose than would be required when the system is supporting a saturated market in a steady state. For a system growing at a rate of 10% per month, an allocation of 40% would allow each ACM in the queue to be exposed to its new authorisations at least 6.7 times as often as the ACMs receiving monthly rekeys in the background. When the population reaches a steady state, a 10% allocation for this kind of traffic is a typical figure.

The system is relatively insensitive to channel bit error rate. At a C/N of 9.5 dB in a D-MAC system, or 8.5 dB in a D2-MAC system, which corresponds to a subjective threshold for acceptable audio quality for level 2 compounded audio, the duobinary bit error rate is approximately 10^-3. Population capacity is always calculated based on this error rate. EMMs are Golay-encoded, which implies an informational bit error rate of approximately 10^-8. In Eurocypher, by using optimal message formats for updating monthly keys, the expected message error rate at threshold, therefore, is about 3.7*10^-6. Thus, so long as the receiver is listening to a Eurocypher channel at the time a message is sent, it will with very high probability correctly receive an update for the monthly key on the first transmission. The probability that a listening receiver in a population of 100 million receives no EMMs broadcast during the month correctly is 6*10^-35.

The most likely reason that an ACM will not receive a rekey message is that the receiver is not listening to a Eurocypher channel at the right times - that is, due to low coverage. The population figures quoted above assume levels of coverage of 85% or better. Even with a coverage of only 60% or better, the 120 kbps control channel can support a population of 50 million subscribers.

Actual coverage statistics are unknown, and will depend both on consumer behaviour and on the number of channels watched which also carry Eurocypher authorisation data. Knowledge of these parameters will improve as the system grows. Therefore, in the early years of system operation, the bandwidth reservation, while apparently excessive for a population of a few million subscribers, provides a safety valve which allows for successful operation even if the assumptions that underlie the analysis of a large system prove to be incorrect.

A number of strategies exist to support operation of over-air addressing implementation in which a significant portion of the population operates at a low level of coverage for one reason or another:

- With appropriate upgrades to the SAS, priority queues can be built

which distribute rekey messages according to known patterns of failure to receive updates. Distribution strategies can thus be modified by consumer behaviour.

- Rights to distribute Eurocypher EMMs over non-Eurocypher channels can be negotiated.

- The period of the validity of EMM-delivered keys can be extended.

- Shared addressing techniques can be used, provided appropriate steps are taken to ensure that the security of the system is maintained.

5 SYSTEM SECURITY

The security of the Eurocypher design is based on principles developed for other VideoCipher systems. These systems have been subject to very extensive pirate attacks. As a result of the experience gained in analysing and countering these attacks, VCD has been able to determine the actual nature of various threats to the system, and the relative strengths and weaknesses of many areas of the original VideoCipher II design. The fundamental system design has never been broken, and many of the security threats considered in the original designs of VideoCipher II systems have never materialised. All breaches of the system's security have been based upon weaknesses in the implementation of the decoder security processing. Exploitation of these breaches have all been based on pirate modifications to legitimate decoders.

Based upon analysis of the pirate attacks seen in the United States, a number of upgrades have been made to the system design to enhance its security. These upgrades have been incorporated into the security design for Eurocypher, and into the implementation of the ACM, wherever possible. VCD has a continuing programme to investigate and develop further security enhancements, which can be phased into the system from time to time if appropriate. The technical design of the system's security is only one aspect of a total security programme. Other aspects of maintaining system security include the development of relationships with law-enforcement agencies to identify and prosecute providers and suppliers of illegal equipment; working with programmers and legislators to remove incentives to piracy; and operating electronic counter-measures to detect and defuse pirate technologies. These aspects lie beyond the scope of this paper, but they are at least as important as the system design in maintaining long-term system security.

5.1 Encryption and Authentication

Secure data is delivered encrypted under an exportable proprietary algorithm, which is designed to prevent cryptanalysis or modification of secure data in a timely fashion by an attacker.

A number of authentication techniques are used, including classical techniques. An important feature in the selection of an authentication technique is its ability to prevent forgery. It has proved possible to develop and implement techniques which protect the ACM against modification of access control data even if the key used to authenticate the protected data is known to the pirate. Similar techniques are used to protect against replay of obsolete data and avoidance of deauthorisation commands.

5.2 Key Hierarchy

The ACM follows a hierarchical key structure which is closely related to that employed in the VideoCipher II systems used in the United States. The Eurocypher key hierarchy is based on a set of unit keys which are unique to each ACM. The ACM possesses a large number of unit keys, but, for each ACM, only one of these keys is known to the uplink computer systems at any given time. Each PCS or SAS possesses a key list for ACMs which are authorised by that computer. This key list can be replaced, if it is ever stolen, by another key list which selects different unit keys for the same ACM addresses. The replacement process ensures that a thief cannot use a stolen keylist once it is replaced.

The unit keys are used to authenticate the ACMs' authorisation capabilities. They are also used to deliver securely in EMMs another key, called the category or monthly key. This key is held by all ACMs in a category and is changed periodically at a low rate, typically monthly. Knowledge of a category key does not allow an attacker to alter either the ACM's authorisation rights or the access control requirements for the protected services. If shared addressing is used to save addressing bandwidth, the unit key can also be used to deliver a shared key securely; the shared key in turn is used to deliver category keys securely. Shared keys may be changed from time to time, as required.

The access requirements for each service are protected under a key known as a programme key. This key is delivered securely in ECMs, encrypted under the category key for each category which is able to access the service. The programme key is changed periodically. In the case of the TV service, a programme key may be associated with individual television programmes, so that each programme may be managed as a separately-secured block of time with its separate set of access requirements. An ACM which is authorised to provide access to a programme will be capable of delivering MAC control words to the receiver every 256 frames for the duration of the programme. The receiver can then descramble video and decrypt audio or data using the PRBS generators defined in the MAC specifications.

The key hierarchy described above protects the basic signal transmission path. Similar techniques are used to authenticate and protect ancillary data paths, such as the transmission of secret unit key lists or sensitive IPPV view history data.

5.3 Physical Security

Secure data protection involves both the storage and protection of secret unit data and the delivered unit specific data. Because the ACM is supporting the television industry, it is created in high volumes and is widely distributed. For this reason, the economic incentive for piracy is high, but the ability to detect and trace pirates rapidly is limited. Consequently, the ACM must be designed to provide a degree of both physical and cryptographic security which is unique in commercial applications. All breakages of VideoCipher II system security have been based on exploiting weaknesses in the implementation of the decoding module. As a result of analysing these weaknesses, and of technological advances over the last few years, the customised secure circuitry in the ACM incorporates a number of features to improve the physical security of the system. These are both physical and algorithmic in nature. The protection of the ACM can be upgraded and enhanced from time to time, as new techniques become available.

5.4 Detachable ACMs

It is believed that the security system outlined above will provide a high degree of protection for Eurocypher customers. The Eurocypher system should be expensive and difficult to break, and exploitation of security breaches should be expensive and difficult to mount and sustain. As an additional disincentive to attempted piracy, the Eurocypher system supports an ability to enhance a system's security in a controlled fashion, through the use of detachable ACMs. These ACMs can interact with the receiver through an external serial interface. In order to ensure that this interface does not become an access path for pirate modules, data across the interface is encrypted by the buried ACM using a key known to the detachable ACM and loaded into the buried ACM by the SAS. Thus, the buried ACM always acts as a buried adaptor. The fact that the buried ACM is associated with detachable modules by the SAS ensures that any upgrade of the system security always takes place under the control of the system operators.

While the main function of the detachable interface is to provide an upgrade path for system security, detachable ACMs could be provided for other reasons:

- To provide access to enhanced Eurocypher access control features.
- To provide access to services available only to a second category.
- To provide access to services which are subject to a different access control system.

6 SUMMARY AND CONCLUSIONS

The Eurocypher system is based on a system architecture which has been proved operationally to meet the business needs of programme providers while providing a wide range of features to the consumer in a convenient form. The system has been extensively enhanced to adapt it to provide access control for MAC systems, and to provide consumer features appropriate for the British and European broadcasting environment. System security has been extensively upgraded to take advantage of the hard-won experience gained in fighting piracy of VideoCipher II in the United States.

The system currently fielded for BSB demonstrates only some of the capabilities inherent in the design. Many features, notably IPPV, can be activated in the future. Eurocypher has the ability to meet the needs of a continental European market [Bagenal90] with both national and pan-European programmers. Eurocypher's capabilities and features give it the potential to play a key role in the future development of the European television market.

7 ACKNOWLEDGEMENTS

The authors would like to thank the Eurocypher marketing and engineering staff, both past and present, for all the long hours and hard work they have put into initiating and realising this project since 1986. We would also like to thank the Conditional Access group at BSB, for their support in coordinating our efforts with other developments in the project, and for their valuable comments and suggestions.

8 REFERENCES

[Bagenal90] - P. Bagenal, S. M. Upton, C. J. Bennett: "Operation of Eurocypher Systems: Current Experience and Future Developments" Proc ACSA '90, Rennes, June 1990 (This conference)

[EBU86] - European Broadcasting Union: "Specification of the MAC/Packet Family", EBU3258 Brussels, September 1986, and subsequent amendments

[EEC86] - EEC Directive 86/259/EEC, European Commission, Brussels, 1986

[Stephansen90] - H. Stephansen: "A Flexible MAC/Packet Encoder Interfacing with Any Conditional Access System" Proc ACSA '90, Rennes, June 1990 (This conference)

SYSTÈME DE TÉLÉVISION A PÉAGE À CONTRÔLE D'ACCÈS PLEINEMENT DÉTACHABLE

UN EXEMPLE D'IMPLÉMENTATION :VIDEOCRYPT

Michel **LEDUC**
THOMSON LEREA
BP 20
67403 ILLKIRCH Cedex
FRANCE
Tel : +33 88 67 67 67

TABLE DES MATIÈRES

Les besoins des diffuseurs de programmes ont entraîné dans les années 80 l'apparition de systèmes de télévision à péage en Europe et surtout aux Etats-Unis. L'analyse à posteriori de ces systèmes fait apparaître un certain nombre de problèmes communs à cette première génération de produit :

- faible niveau de sécurité entraînant un taux élevé de piraterie,

- services offerts limités en nombre et en performance,

- systèmes à caractère non évolutif.

L'accroissement sensible de la demande ainsi que les exigences de sécurité demandées en particulier par les concepteurs de programme ont entraîné l'apparition d'une deuxième génération de produits. L'utilisation de la carte à puce au niveau du contrôle d'accès dans un certain nombre de produits a constitué une véritable révolution. Une utilisation optimisée de cette carte à puce a permis d'élaborer un nouveau concept de télévision à péage basé sur un contrôle d'accès totalement détachable. Une première implémentation de ce concept a été réalisée dans le système VIDEOCRYPT.

I- PREMIERE GENERATION

Cette première génération de systèmes fut caractérisée par le regroupement des fonctions suivantes au sein du décodeur :

- fonction de désembrouillage,
- fonction de décryptage,
- fonction de traitement des autorisations.

Ces éléments constituent une cible fixe mise à disposition des pirates éventuels. L'attaque simultanée des techniques d'embrouillage et de cryptage a permis dans de nombreux cas de percer le secret du décodeur et ainsi de le dupliquer. Une fois ce secret découvert, le système entier s'effondre et l'unique parade consiste à remplacer l'ensemble du parc de décodeurs.

Autre conséquence de ce type d'architecture, l'ensemble des services offerts ainsi que leur niveau de performances sont figés à la conception du produit. Le prestataire de services ne peut faire évoluer son offre en fonction de l'évolution des besoins du marché ou de sa stratégie marketing (besoins de services de type nouveau, augmentation de leur quantité ou de leur complexité).

II- LA DEUXIEME GENERATION

Les concepts développés dans cette deuxième génération de systèmes ont essayé de palier avec plus ou moins de réussite les problèmes exposés précédemment, mais il est indéniable aujourd'hui que les systèmes comportant un contrôle d'accès à carte à puce ont permis d'apporter une réponse satisfaisante et ainsi révolutionner la télévision à péage.

III- LES PRINCIPES DU CONTROLE D'ACCES DETACHABLE

En séparant physiquement le module de contrôle d'accès du décodeur et en affectant à ce module l'intégralité des fonctions de sécurité de gestion des autorisations et d'identification de l'abonné, on crée ainsi un système ouvert, flexible et évolutif tant au niveau de la sécurité que des services offerts. Une utilisation judicieuse de la carte à puce permet de réaliser ce type de contrôle d'accès.

III.1. l'architecture du système : voir annexe

- rôle du décodeur

  Canal de données transparent : après extraction des données (de la vidéo par exemple), le décodeur se contente de vérifier que ces données ne contiennent pas d'erreur puis sans autre traitement, il les transmet INTEGRALEMENT au module de contrôle d'accès détachable (c'est-à-dire la carte).

  Désembrouillage: Dans le cas où le contrôle d'accès l'autorise, le décodeur désembrouille le signal vidéo à partir des données reçues.

  Gestion de l'interface utilisateur :

- rôle du contrôle d'accès détachable

  . identification de l'abonné,

  . gestion des autorisations,

  . identification de l'opérateur (cas des systèmes multiopérateurs),

  . gestion de la diffusion des messages et de leur niveau de priorité,

  . tri et sélection des données,

  . processing de l'algorithme de décryptage et transmission du "seed" (de la graine) pour le désembrouillage,

  . processing de l'algorithme d'authentification du module lui-même.

III.2. Avantages de ce type d'architecture

- une sécurité optimale :le système constitue une cible mouvante pour les pirates:

. l'algorithme utilisé n'est ni unique, ni figé. Il appartient à une famille d'algorithmes et on peut en changer à volonté simplement en remplaçant la carte.

. la complexité de l'algorithme et la complexité de la carte peuvent être adaptés au besoin et à la durée de vie du service offert (utilisation de carte "bas coût" dont la durée de vie est limitée à la durée d'un événement).

. le décodeur ne contient aucun secret, sa duplication ne comporte aucun intérêt.

. le procédé d'identification des cartes assure que les cartes utilisées sont valides et empêche la création éventuelle de "fausses cartes" avec des numéros d'identification diversifiés.

- une grande ouverture et une grande flexibilité du système

. possibilité d'accroître le nombre et la complexité des services offerts en utilisant une carte plus puissante ; la structure interne de la carte peut être adaptée aux besoins spécifiques de l'application ;

. possibilité d'implanter de nouveaux services au moment opportun sans même l'avoir prévu à l'époque de l'implantation du système ;

. la ou les méthodes d'adressage ne sont pas figées et peuvent évoluer avec le système (adressage groupé, statistique) ;

. possibilité de faire profiter le système des évolutions technologiques (nouvelles cartes à puce avec mémoire plus large ou avec mémoire réinscriptible) ;

. pas de syntaxe déterminée dans le flot de datas transmises, ce qui permet d'envisager une optimisation de leur utilisation en fonction de l'application requise.

. le décodeur ne possédant pas d'élément d'identification, une carte peut être utilisée dans n'importe quel décodeur.

IV. EXEMPLE D'IMPLEMENTATION

Le système VIDEOCRYPT constitue la première implémentation d'un système de télévision à péage à contrôle d'accès pleinement détachable. Plusieurs réalisations à travers le monde dont la première, SKY télévision, ont permis de mettre en évidence les avantages de ce type d'architecture. Pour constituer un des systèmes les plus robustes et le mieux adapté à ce type de marché, le système Videocrypt allie les concepts suivants:

- concept de contrôle d'accès pleinement détachable,

- concept d'embrouillage basé sur l'inversion de ligne à un point de coupure,

- concept de voie de données à faible débit et haute sécurité.

IV.1. Concept d'embrouillage vidéo :

Le principe d'embouillage discret 2 a été adapté de manière à pouvoir être utilisé de façon transparente quels que soient les médias de transmission, c'est-à-dire aussi bien les transmissions par câble, réseaux terrestres, MMDS, fibre optique ou satellite. De même, Videocrypt s'adapte à tous les standards vidéo, PAL SECAM NTSC ou autre...

IV.1.1. Le principe :

Un point de coupure est défini dans la partie active de chaque ligne visible d'une image ; ce point définit donc un segment gauche et un segment droite. L'embrouillage consiste donc à permuter ces deux segments autour du point de coupure, le segment de droite passant à gauche et celui de gauche à droite.

La position du point de coupure est donnée par un générateur pseudo-aléatoire dont l'information est chargée à chaque ligne. Ce générateur pseudo-aléatoire est réinitialisé périodiquement en synchronisme avec l'émission au moyen d'un mot de contrôle. Dans l'implémentation actuelle de SKY television, le mot de contrôle a une largeur de 60 bits et on le transmet dans la voie de données toute les 2.5 secondes, le nouveau protocole Vidéocrypt permet de réduire l'intervalle de temps entre deux mots de contrôle à 0.6s.

IV.1.2. Les particularités :

Pour offrir les meilleures garanties de sécurité et de conservation de la qualité de l'image, le système d'embrouillage de Videocrypt incorpore les particularités suivantes :

- un point de coupure indétectable dans la video transmise grâce à une technique judicieuse d'interpolation permettant d'atténuer la transition à la jointure des deux segments.

- un point de coupure indétectable dans l'image reconstituée après désembrouillage grâce à des techniques adéquates de recouvrement et de jitter-free. Aujourd'hui même l'emploi de techniques sophistiquées telles que la corrélation horizontale et verticale n'a pu permettre de venir à bout d'une manière fiable de ce type d'embrouillage.

- un point de coupure choisi parmi plusieurs centaines dans la partie active de la ligne vidéo.

- un concept d'embrouillage qui ne touche pas aux éléments de synchronisation.

- un concept d'embrouillage qui conserve son intégrité à la video transmise et qui ne requiert aucune modification des moyens de transmission (émetteur, réémetteur, tête de réseau, etc). Le signal vidéo une fois désembrouillé reste parfaitement conforme aux normes CCIR.

- un concept d'embrouillage qui assure une parfaite confidentialité de l'image transmise. Il est, en effet, parfaitement impossible d'en deviner le contenu. Cependant des modes appropriés permettent de diminuer partiellement cette confidentialité pour des opérations de promotion.

IV.1.3. Les modes de fonctionnement :

Le système offre les modes de visualisation suivants :

- mode clair,

- mode semi-embrouillé dit mode mosaïque,

- mode embrouillé à accès libre (c'est-à-dire avec un mot de contrôle fixe. Dans ce cas, il suffit de posséder un décodeur pour avoir accès au programme),

- mode embrouillé à accès contrôlé : dans ce cas une carte à puce dûment autorisée est indispensable pour accéder aux programmes.

IV.2. Le canal de données

Une des particularités attrayantes du système à contrôle d'accès pleinement détachable tel qu'il est implémenté dans le système Videocrypt, est de ne pas requérir un débit élevé au niveau du canal de données tout en garantissant des capacités d'adressage élevées. Ceci nous a permis de définir un canal de données extrêmement robuste qui peut s'affranchir des aléas de transmission et ainsi garantir le désembrouillage de l'image et la réception des autorisations même dans le cas de conditions de réception délicates.

IV.2.1. Principe :

Le canal de données de type Vidéocrypt utilise 4 lignes de l'intervalle de retour trame. Le choix de ces lignes n'est pas figé et peut se faire en commun avec l'opérateur de programme.

Le débit instantané est de 800 Kb/s ce qui, avec l'adjonction de trois niveaux de protection dont un codage de Hamming et la répétition multiple des paquets de données, permet de ne transmettre au contrôle d'accès que des données valides.

IV.2.2. Performances :

Le canal de données ainsi défini permet de s'affranchir des problèmes de transmission et en particulier dans les cas de conditions de réception délicates. Son immunité aux phénomènes courants de transmission tels que échos, ghost a pu être démontrée dans de nombreux essais ; même lorsque le signal transmis est bruiteux ou très faible les données sont encore parfaitement transmises. Ainsi avec un niveau de C/N de 3db pour une transmission satellite ou encore lorsqu'un récepteur de télévision perd la couleur et que l'image reçue n'est même plus regardable, le signal est toujours désembrouillé et les autorisations reçues.

IV.3. L'embrouillage du son :

La très grande sécurité offerte par l'utilisation de la carte à puce et par le concept d'embrouillage vidéo choisi permet d'associer un son non embrouillé conférant un aspect attractif au programme embrouillé transmis vu la parfaite confidentialité de la vidéo transmise. Une large gamme de concepts d'embrouillage son plus ou moins confidentiels ou plus ou moins sécuritaires peut aussi être proposée dans le cadre du système Vidéocrypt :

- son coupé : son supprimé lors d'un programme embrouillé (utile dans le cas de récepteur/décodeur intégrés),

- inversion de spectre simple,

- inversion de spectre à porteuse variable,

- son digital de type NICAM embrouillé : ce concept offre les mêmes garanties de sécurité et de qualité de transmission que l'embrouillage vidéo, il peut utiliser une fonction dérivée du mot de contrôle transmis pour la vidéo ou encore son propre mot de contrôle.

IV.4. Le contrôle d'accès

Le contrôle d'accès à caractère pleinement détachable implémenté dans le système Videocrypt se différencie des autres systèmes connus dans les domaines suivants :

* Sécurité et flexibilité :

- aucun secret dans le décodeur ; toutes les autorisations, tous les algorithmes, les numéros d'identification résident dans la carte,

- la carte réalise en permanence un contrôle de validité. Un algorithme contenu dans la carte permet de réaliser une authentification de la carte sur demande de l'émetteur et ceci sans que la carte ne transfère aucune connaissance au décodeur. Les algorithmes employés sont appelés "zero knowledge transfert algorithme",

- les cartes et par conséquent l'ensemble de leur contenu peuvent être changées périodiquement ; ainsi le système ne se comporte pas comme une cible fixe pour les pirates éventuels,

- l'algorithme de décryptage des mots de contrôle n'est pas unique, il appartient à une famille d'algorithme. De plus, il opère sur l'ensemble des données transmises.

* Services offerts :

La très grande souplesse du système ne permet pas de dresser une liste exhaustive des services offerts cependant on peut citer les possibilités suivantes :

* Paiement à la séance ou pay-per-view et ceci dans tous les modes connus. Il est à noter que les opérations de débit et de crédit sur la carte peuvent se faire "over the air" grâce à la sûreté et à la sécurité du transfert des informations,

* Abonnement périodique

* Abonnement par thème

* Abonnement par programme

* Carte pour un seul événement : le système Vidéocrypt permet d'utiliser des cartes dites "faible coût" du type cartes téléphoniques utilisées en France. Comme exemple d'application, on peut considérer la sponsorisation d'un événement sportif, les cartes étant distribuées gratuitement au cours d'une opération de promotion d'un produit. Ce type de carte ne contenant que de l'Eprom, leur protection est réduite mais leur durée de validité est bien évidemment réduite à la durée de l'événement lui-même.

* TV achat, pari etc : l'utilisation combinée du procédé de signature et de la sécurité de l'identification de la carte permet d'envisager de multiples applications dont le TV achat et des systèmes de promotion ou de pari.

* Messagerie : Videocrypt offre aux prestataires de service des possibilités de messagerie sécurisée et hiérarchisée. Ces messages pourront être transmis de manière individuelle, groupée ou globale.

De nouveaux services, éventuellement des services dont le principe n'a pas été encore élaboré pourront être implémenté sans pour cela remettre en cause le parc de décodeur. Il suffira de créer une nouvelle carte avec le logiciel adapté et de modifier en conséquence le logiciel du centre de gestion.

IV.5. Le terminal lui-même :

Malgré la sophistication du traitement digital de la vidéo et du traitement des informations pour la carte à puce, un décodeur Videocrypt peut conserver une architecture simple et être réalisée avec des composants grand public et des techniques de réalisations grand public.

On décompose le terminal en trois parties :

- Interfaces entrées/sorties : elles varient suivant l'application concernée et peuvent inclure :

    * Tuner satellite, terrestre ou câble

    * Modulateur

    * Interface péritélévision (simple ou multiple avec régie son et vidéo)

    * Télécommande infra-rouge

    * Clavier

    * Modem ou plus généralement une interface de voie de retour

    * etc

- Le désembrouillage vidéo : il est architecturé autour d'un chip spécifique qui commande deux buffer de ligne afin de remettre dans le bon ordre les échantillons de vidéo digitalisés au moyen d'un convertisseur A/D 8bits.

- Gestion du décodeur et gestion du dialogue avec la carte.

Un premier microcontrôleur gère les interfaces entrées/sorties et réalise l'interface utilisateur sous mode menu. Ce microcontrôleur traite les données extraites de la vidéo et s'assure de leur intégrité avant de les transmettre au deuxième microcontrôleur.

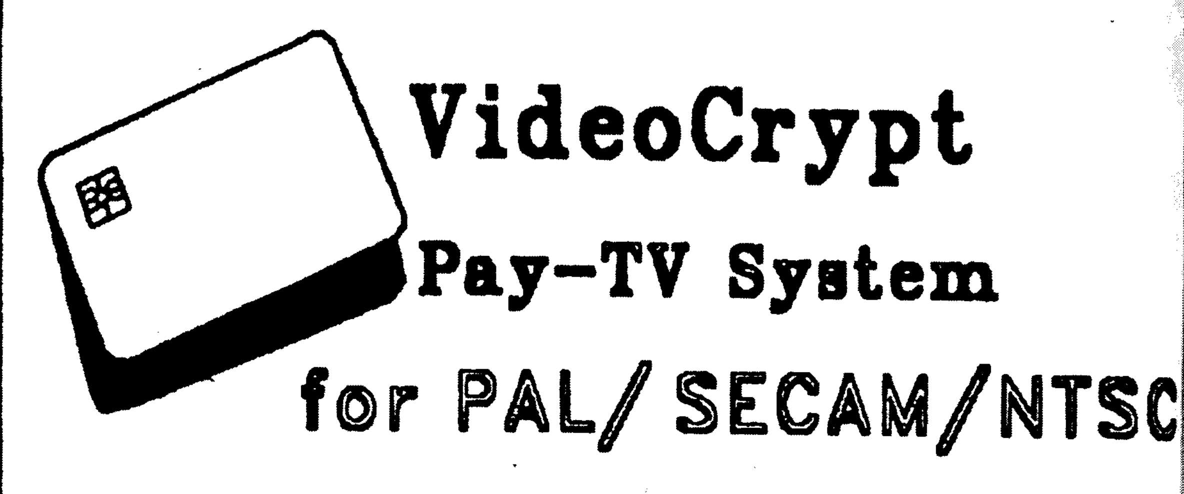
Le deuxième microcontrôleur appelé "Verifier" gère le dialogue avec la carte à puce.

CONCLUSION :

La grande innovation offerte par ce type d'interface réellement et pleinement détachable ouvre de nouvelles voies aux prestataires de services.

Le système peut s'adapter au fur et à mesure des besoins à la stratégie du prestataire de services sans remettre en cause son investissement.

Par ailleurs, les décodeurs Vidéocrypt sont ouverts vers de futures évolutions technologiques. Dès aujourd'hui, ils sont réalisés dans des technologies grand public ce qui leur permet d'atteindre des dimensions et un coût attractif. L'intégration en un seul chip du coeur du système en phase de test aujourd'hui permet d'envisager un module réalisant la fonction Vidéocrypt dans des dimensions lui permettant d'être implémenté aisément dans n'importe quel produit grand public (TV, magnétoscope, récepteur satellite, etc) ou professionnel.



EMITTER SIDE

RECEIVER SIDE

Encryption

Scrambling

De-Scrambling

Decrypti

CLEAR VIDEO

SCRAMBLER

CONTROL DATA

ENCRYPTER

DATA INSERTER

SCRAMBLED VIDEO

CONTROL DATA OF SCRAMBLING PROCESS

DE-SCRAMBLER

DATA RETRIEVER

CLEAR VIDEO

SECU MODU

EMMITTER SIDE # SCRAMBLING **RECEIVER SIDE**

LINE CUT & ROTATE

CLEAR VIDEO

CONTROL DATA

SCRAMBLED VIDEO + CONTROL DATA

61-bit PRBS GENERATOR

61-bit PRBS GENERATOR

CLEAR VIDEO

THOMSON CONSUMER ELECTRONICS

DATA CHANNEL

4 Data Lines

White Test Line

Black Test Line

Vertical Blanking Interval (VBI)

Scrambled Video

- 800 Kb/s (instantaneous)
- NRZ coding
- 3 levels of error-protection

THOMSON CONSUMER ELECTRONICS





SUBSCRIPTION VIEWING CARD

MICROPROCESSOR-BASED

"SINGLE-EVENT" CARD

SIMPLE MEMORY

VideoCrypt services :

* SUBSCRIPTIONS
* PAY-PER-VIEW
* INTERACTIVE TV GAMES
* TELE-SHOPPING

TAXINOMIE ET TYPOLOGIE
DE L'ACCÈS CONDITIONNEL

Louis Claude GUILLOU
CCETT
4 rue du Clos Courtel, BP 59
35512 CESSON SEVIGNE Cedex
FRANCE
Tél : +33 99 02 41 11

Jean-Jacques QUISQUATER
Philips Research Laboratories
2 avenue Van Becelaere
B-1170 BRUXELLES
BELGIQUE
Tél : +32 2 674 2243

RÉSUMÉ

Cet article cherche à modéliser l'accès conditionnel en diffusion. Après un positionnement du sujet précisant en quoi consiste l'accès conditionnel, deux modèles sont présentés :

- Un modèle à distribution des mots de contrôle illustre ce qui est exploité aujourd'hui par Canal Plus.
- Un modèle à distribution d'autorisations illustre ce qui est mis en œuvre dans le cadre d'Eurocrypt.

Cette modélisation fait ressortir l'impact de la normalisation et les possibilités d'évolution.

ABSTRACT

This paper aims at a modelisation of conditional access in broadcast environment. After defining the subject by saying what is conditional access, two models are presented.

- Control words are distributed in a model which illustrates what is used by Canal Plus.
- Authorisations are distributed in a model which illustrates what is developed to-day for Eurocrypt.

This modelisation emphazises the impact of standardization and the reserves for further evolution.

TABLE DES MATIÈRES

2.3 Rôle des mots de contrôle

Les mots de contrôle, une fois déchiffrés, servent à définir l'état initial des automates produisant les séquences nécessaires au désembrouillage de l'image (pour chaque ligne, l'adresse d'un point de coupure parmi 256 points possibles) et du son (pour chaque paquet de données sonores, un motif déchiffrant à combiner par ou-exclusif au contenu du paquet). L'attaque brutale des composantes diffusées devient assez peu économique, surtout pour les sons.

Le même mot de contrôle est utilisé de la même manière au niveau du point d'émission pour les opérations d'embrouillage et au niveau de chaque décodeur pour les opérations de désembrouillage.

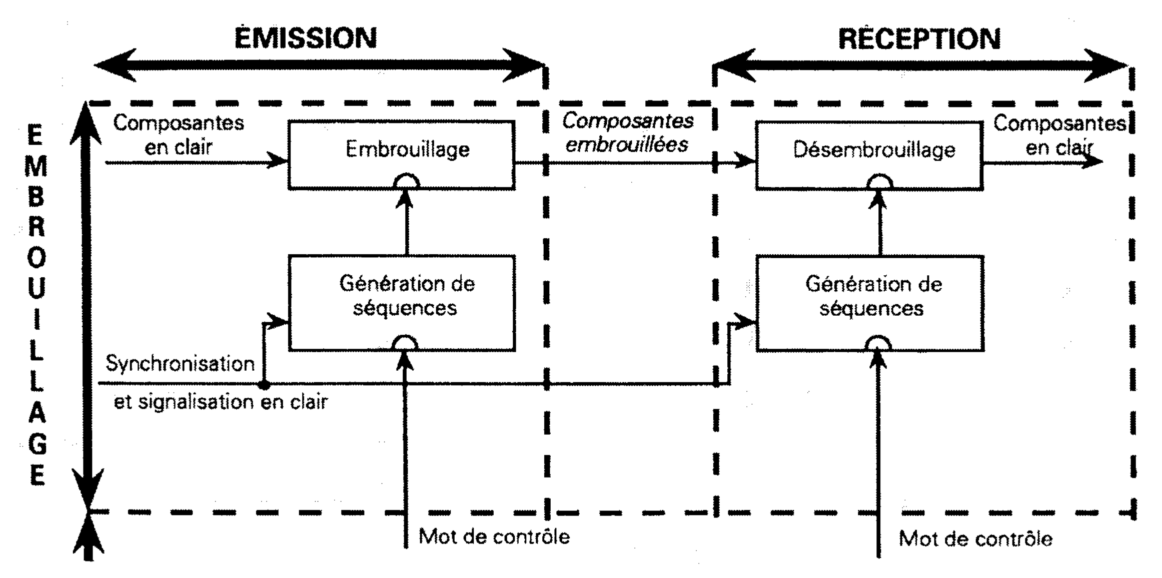


FIGURE 1 — Embrouillage des composantes

L'accès au programme se trouve donc ramené à l'accès à des mots de contrôle qui servent à mettre à la clé les opérations de désembrouillage dans les décodeurs des usagers. La suite de l'article porte exclusivement sur la manière d'accéder à ces mots de contrôle et sur la manière de gérer l'audience afin de minimiser : — les contraintes imposées à l'usager, — les coûts de gestion et — la fraude.

On ne peut pas dire qu'il y ait une évolution du plus simple au plus complexe. Il y a simplement des optimisations économiques liées à l'état général des outils disponibles à un moment donné, compte tenu de l'évolution technologique.

3 Modèle à distribution des mots de contrôle

Ce modèle est utilisé aujourd'hui par Canal Plus en France.

Chaque mois, chaque abonné reçoit un courrier personnalisé qui lui indique un code à frapper au clavier du décodeur pour le mettre à la clé pour le mois suivant.

Dans le cœur du décodeur, un microcalculateur reconstitue un mot de 16 bits à partir du cryptogramme frappé au clavier par l'usager. Ce mot est le mot de contrôle évoqué au paragraphe précédent.

Le code frappé au clavier est en fait un cryptogramme du mot de contrôle. En effet, chaque décodeur est individualisé par une clé de distribution qui varie d'un décodeur à l'autre. Cette clé de distribution paramètre un algorithme cryptographique exécuté par le microcalculateur du décodeur pour rétablir le mot de contrôle en déchiffrant le cryptogramme. Cet algorithme n'est pas publié. Sa sécurité logique est aussi un des facteurs déterminants de la sécurité globale du système.

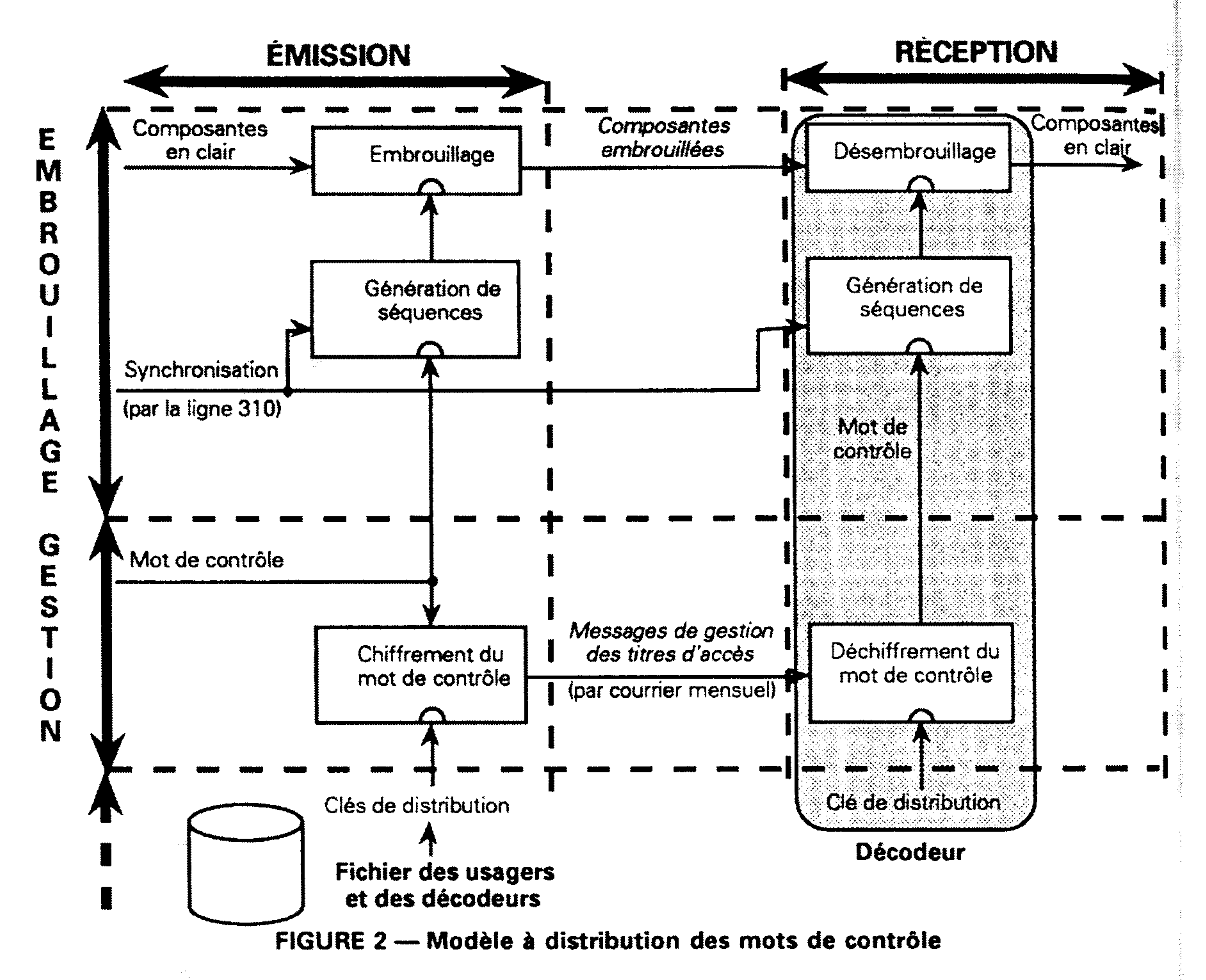


FIGURE 2 — Modèle à distribution des mots de contrôle

Notons quelques conséquences au niveau de la gestion du système.

— La sécurité physique des décodeurs est un autre élément important de la sécurité globale du système. Les décodeurs sont immatriculés et identifiés ; un fichier des usagers établit la relation entre décodeurs et usagers. Les décodeurs sont loués avec le service : ils restent la propriété du gérant du système. La fabrication et la réparation des décodeurs doivent être contrôlées. Il faut mettre à jour le fichier des usagers à tout remplacement de décodeur défectueux.

— Il n'est pas envisageable d'intégrer de tels décodeurs dans les téléviseurs de l'avenir.

— Les décodeurs sont dédiés à un service ; en cas de multiplication des services payants, on doit envisager en poursuivant cette solution de multiplier les décodeurs, ce qui est inacceptable pour les usagers.

— Les codes mensuels ne doivent pas être longs, car les usagers doivent les frapper sur le clavier de leur décodeur.

NOTE — On pourrait bien sur envisager d'autres moyens de saisie des codes mensuels : codes à barres, tickets magnétiques, ... mais cela n'est pas compatible avec les impératifs de coût du décodeur.

Il y a tout de même une certaine harmonie du produit développé par Canal Plus : la sécurité physique du décodeur est à la mesure de la résistance des techniques d'embrouillage. En effet, on ne met pas une serrure de haute sécurité sur une porte facile à contourner. La résistance fort limitée du produit a induit le législateur à pénaliser la détention de boites pirates, donc à plus forte raison leur fabrication et leur commerce. Malgré tout, ces choix ont permis à une chaîne à péage de voir le jour et de se développer en gagnant de l'argent.

4 Modèle à distribution des autorisations

Quand la diffusion comporte une indication de synchronisation telle qu'un compteur de trames, alors cette information peut être utilisée pour produire les mots de contrôle. Une fonction à sens unique, facile à calculer, mais difficile à inverser, est utilisée pour générer les mots de contrôle. L'un des arguments de la fonction à sens unique est une clé d'autorisation de base. Le qualificatif «de base» signifie qu'il ne peut y avoir qu'une clé de ce type en usage à un moment donné sur un service donné.

Cette possibilité est prise en compte dans les spécifications produites par l'UER. Un nouveau mot de contrôle est produit toutes les 256 trames (environ 10 secondes) à partir des 20 bits de poids fort du compteur de trames.

Les spécifications produites par l'UER prévoient aussi un mot de contrôle local qui permet de tester facilement divers équipements. Cependant, l'embrouillage systématique n'a pas été imposé. Un tel embrouillage systématique augmenterait d'environ 1,5 décibel l'isolation entre canaux en réduisant les effets de diaphotie.

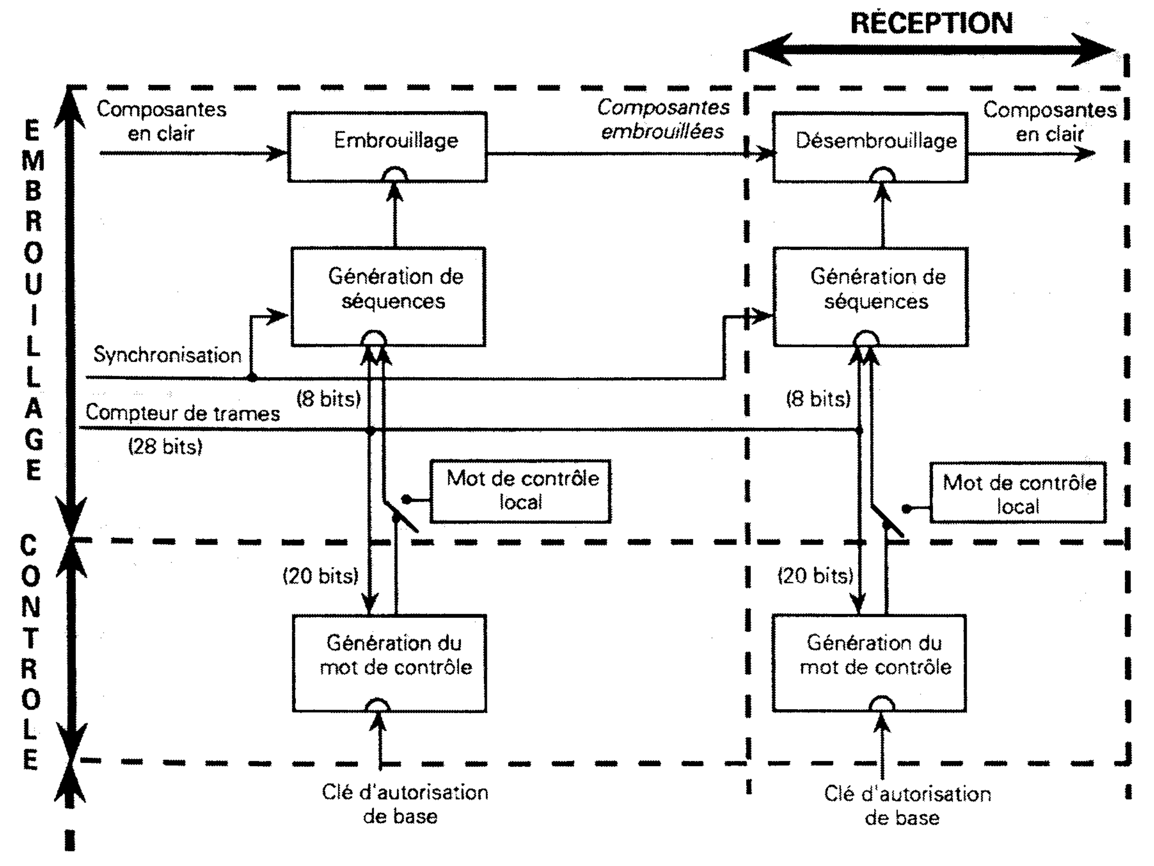


FIGURE 3 — Modèle à distribution des autorisations avec ECM implicites

Quand le système permet de diffuser des messages de service pour un coût marginal, en multiplexage avec les composantes embrouillées, alors les mots de contrôle sont tirés au hasard à l'émission, puis chiffrés grâce à un algorithme de chiffrement utilisant une clé d'autorisation, et déchiffrés à la réception au niveau du décodeur par un algorithme de déchiffrement utilisant la même clé d'autorisation. Les messages de service sont appelé «messages de contrôle des titres d'accès» (en anglais 'entitlement control messages' abrégés en ECM)). Le mot de contrôle (en anglais 'control word' abrégé en CW) peut alors être à la fois long en information (une soixantaine de bits) et bref en durée de vie (quelques dizaines de secondes). Des microcalculateurs de sécurité matérialisent les titres d'accès des usagers et rétablissent les mots de contrôle à partir des messages de contrôle.

Il faut bien sur mettre à jour les titres d'accès des usagers dans leurs microcalculateurs de sécurité. Pour modifier les titres d'un usager, il faut que le microcalculateur de sécurité de l'usager reconnaisse la voix de son maître. Le microcalculateur utilise une clé de distribution pour vérifier les «messages de gestion des titres d'accès» (en anglais 'entitlement management messages' abrégé en EMM). Quand le résultat du calcul cryptographique est cohérent, le microcalculateur persuadé d'avoir affaire à son maître exécute les opérations requises pour gérer les titres d'accès.

Les messageries de gestion des titres d'accès peuvent être partagées entre plusieurs usagers de manière à réduire le nombre de bits utilisés pour chaque usager. Un groupe d'usagers doit alors partager la même clé de distribution.

Ainsi parvient-on au modèle d'accès conditionnel décrit dans la figure suivante, très proche de celle publiée par l'Union européenne de radiodiffusion (UER).

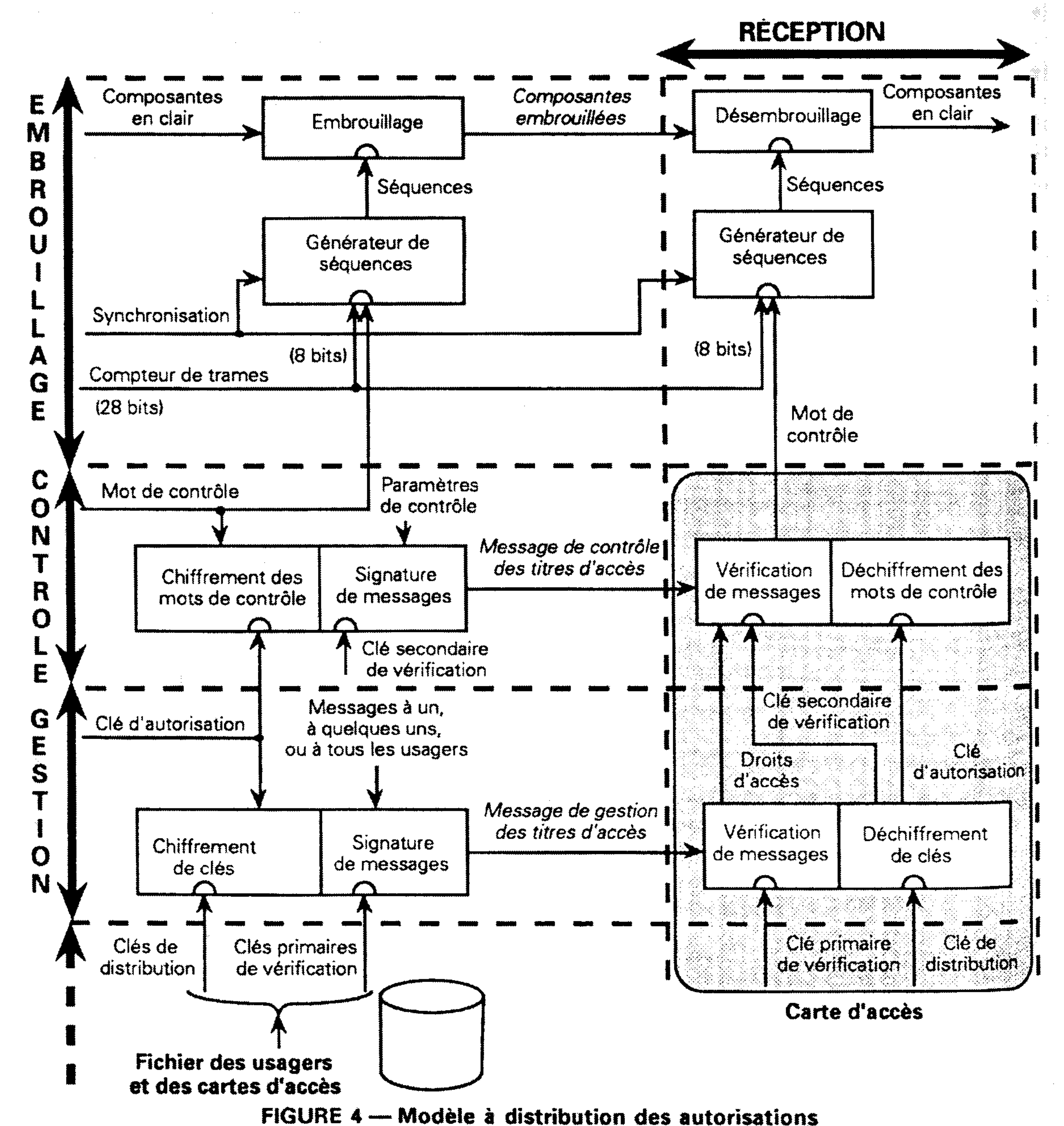


FIGURE 4 — Modèle à distribution des autorisations

4.1 Titre d'accès : clé ou droit d'utiliser une clé ?

Mais qu'entend on par titre d'accès ? Deux positions se sont affrontées à l'UER.

Première position : Tous ceux qui détiennent la même clé de service ont le même droit. Cette position simple à expliquer complique la gestion. Pour modifier l'état d'un seul usager, il faut modifier la clé d'autorisation : cela implique tous les autres usagers. La gestion d'une partie de l'ensemble implique la gestion de l'ensemble.

Quand le changement de clé d'autorisation se fait par adressage à l'antenne, la nouvelle clé est distribuée à des pirates éventuels qui auraient fait des clones d'un microprocesseur de sécurité et qui continueraient à payer les droits pour le microcalculateur original. En changeant de clés de service à tout bout de champ, on ne modifie pas la sécurité d'un tel système.

C'est la confusion entre la gestion des clés d'autorisation et la gestion des titres d'accès au service qui entraîne une gestion "totalitaire" du système : toute modification de l'audience, aussi minime soit-elle, implique la totalité de l'audience.

Deuxième position : un titre d'accès est défini par un état restreignant l'usage d'une clé d'autorisation. Cet état est géré carte par carte, sur une base individualisée. Plus complexe au premier abord, cette proposition simplifie en fait la gestion du système.

Pour modifier les titres d'un usager, il suffit de modifier l'état d'utilisation d'une clé d'autorisation dans le microcalculateur de sécurité de l'usager. Seule la partie concernée de l'audience est affectée par cette gestion "individuelle".

L'adressage à l'antenne est principalement réservé à la gestion d'états associés aux clés d'autorisation dans les microcalculateurs de sécurité. Ainsi, par exemple, on peut renouveler un abonnement, inscrire une séance payée à l'avance, distribuer de nouveaux crédits sous la forme de tickets à consommer ...

Cette réflexion est confortée par l'analyse suivante.

— D'une part, la gestion de la clé d'une autorisation est un problème de confidentialité, où le microcalculateur de sécurité est mis à la clé. La gestion des clés implique la mise en œuvre de secrets. La normalisation d'une technique de mise à la clé est peu probable aujourd'hui, compte tenu des problèmes politiques soulevés par cette question.

— D'autre part, la gestion de l'état d'une autorisation est un problème d'intégrité, où le microcalculateur de sécurité doit reconnaître son maître. La gestion de l'état n'implique pas obligatoirement le secret, et quelques solutions techniques apparaissent dans cette direction. La normalisation de techniques de gestion de droits sans secret pour l'usager ne soulève pas les mêmes problèmes politiques, dans la mesure où on ne peut détourner l'usage de ces techniques qui ne permettent pas la mise à la clé.

4.2 Microcalculateur de sécurité : enterré ou bien détachable ?

Le microcalculateur de sécurité doit rester la propriété du gérant du système. Quand, de manière imagée, on dit qu'il reconnaît son maître, cela illustre bien que ce ne sont pas les souhaits de l'usager, mais bien les ordres du maître, qui doivent être pris en compte. Toute solution doit s'appuyer sur des dispositifs présentant des garanties suffisantes de sécurité physique.

Si le microcalculateur de sécurité est enterré dans le décodeur, alors le décodeur lui-même doit rester la propriété du gérant du système. Nous avons évoqué les conséquences de cette situation sur la fabrication, la vente et la réparation des décodeurs. Un décodeur ne peut avoir deux maîtres à la fois. Au fur et à mesure que les chaînes à péage se multiplient, il faut alors multiplier les décodeurs.

Si le microcalculateur de sécurité est détachable, alors les décodeurs peuvent être banalisés. La fabrication, la vente et la réparation en sont libres. On peut même envisager de les intégrer dans les téléviseurs. Mais il faut en conséquence mener à bien un travail supplémentaire en normalisation en prescrivant l'interface entre le décodeur et le microcalculateur de sécurité.

Vaut-il mieux décrire en détail un algorithme cryptographique sans trop savoir sur quel microcalculateur de sécurité il sera implanté, ou bien décrire l'interface d'une famille de microcalculateurs de sécurité sans dévoiler les algorithmes cryptographiques utilisés ?

La possibilité d'évolution des solutions est un facteur déterminant dans le choix de la solution : les microcalculateurs de sécurité détachables permettent l'évolution des masques de programmes (en particulier les algorithmes cryptographiques et les modes de commercialisation des services qui sont en fait les méthodes d'utilisation des algorithmes) et même l'évolution des microcalculateurs eux-mêmes.

4.3 Cartes à puce

Le contrôle d'accès à distribution d'autorisations avec une carte à puce a été conçu et développé au CCETT avant même que Canal Plus ne soit créé, et que l'UER et l'ISO n'entament leurs travaux de normalisation. Aux actes d'un congrès à Liège en Belgique le 24 novembre 1980, figure un article écrit par Louis Guillou sous le titre «*Radiodiffusion à péage pour application au télétexte ANTIOPE*».

Aujourd'hui, les magazines Chronoval et Chronoptions sur ANTIOPE fournissent chaque jour en France diverses informations boursières commercialisées par la société SDIB. Les mots de contrôle ont une longueur de 60 bits et une durée de vie de 20 secondes. Les cartes à puce PC0 fonctionnent sur la base d'un abonnement mensuel.

Cependant, il a fallu attendre les normes D2-MAC paquet pour transposer efficacement le procédé à la télévision. Le système «Visiopass» est une évolution du système spécifié pour ANTIOPE. Les cartes PC2 font place aux cartes PC0. Et le procédé est adapté à la télévision en D2-MAC paquet.

L'organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) prescrivent l'interface des cartes à microcircuits à contacts dans la série de normes *ISO/CEI 7816, Cartes à circuits intégrés à contacts*. L'interface entre les décodeurs «Visiopass» et les cartes PC2 contenant les titres d'accès des usagers est conforme à cette série de spécifications.

— *ISO/CEI 7816/1*, 1987, *Caractéristiques physiques*.

— *ISO/CEI 7816/2*, 1988, *Dimensions et emplacements des contacts*.

— *ISO/CEI 7816/3*, 1989, *Signaux électroniques et protocoles d'échange*.

Note — Les microcalculateurs pour cartes à puce sont de sérieux candidats comme microcalculateurs de sécurité, que leur utilisation soit prévue comme dispositifs enterrés ou comme dispositifs détachables.

Dans ces systèmes utilisant des cartes à puce, on distingue

— les cartes mères utilisées par les gérants des services pour élaborer les ECM (cryptogrammes des mots de contrôle) et les EMM (distribution de nouvelles clés d'autorisation ; gestion de droits associés à une clé d'autorisation) ;

— les cartes filles utilisées par les usagers des services pour reconstituer les mots de contrôle et matérialiser les droits d'accès.

Dans les cartes PC2, les messages proposés aux cartes filles pour entreprendre un calcul de contrôle ou une opération de gestion ont tous la même structure.

— Un premier champ d'information précise à qui s'adresse le message : à toutes les cartes à la fois, à un groupe de cartes avec une indication oui/non pour chaque carte du groupe, ou à une carte, ainsi que le but de l'opération : calcul d'un couple de mots de contrôle, distribution d'une nouvelle clé d'autorisation, ou attribution d'un nouveau droit.

— Un deuxième champ contient : deux cryptogrammes, un cryptogramme, ou rien du tout, suivant le but de l'opération : deux mots de contrôle, une clé d'autorisation, ou une gestion de droit.

— Un troisième champ porte un code d'authentification de l'ensemble du message.

La carte commence par vérifier le code d'authentification du message avant d'entreprendre toute autre action. Quand le code n'est pas cohérent, la carte devient muette. Il faut ensuite la remettre à zéro pour pouvoir à nouveau dialoguer avec elle. En pratique, les cartes filles PC2 se comportent donc en fonctions nulles presque partout quand on leur soumet des messages pris au hasard. La densité des messages entraînant un calcul est d'environ un message tous les 2^{64} messages puisque chaque code d'authentification de message comporte 64 bits.

Dans les cartes PC2, les clés utilisées pour la vérification de codes d'authentification de message sont distinctes des clés utilisées pour déchiffrer des cryptogrammes contenus dans ces messages.

En outre, il faut fournir en cartes filles plusieurs gérants de services sans qu'il y ait d'interférence entre la sécurité des uns et des autres. De plus une même carte fille doit pouvoir supporter des droits pour des gérants de services différents sans qu'il y ait d'interférence dans la carte entre les secrets des uns et les secrets des autres. L'architecture des cartes PC2 est donc organisée en une «entité maîtresse» (en anglais 'master file' abrégé en MF) et en plusieurs «entités dédiées» (en anglais 'dedicated file' abrégé en DF). L'objectif de sécurité est d'assurer l'étanchéité entre les diverses entités dédiées, et aussi entre l'entité maîtresse et les entités dédiées. À l'ISO, ces sujets sont aujourd'hui en cours de normalisation en vue de l'établissement d'une quatrième partie à la norme ISO/CEI 7816.

5 Évolution des cartes et des décodeurs

La télévision à péage acquiert aujourd'hui une dimension européenne. La diversité des solutions présentées au cours de ces journées est plutôt une garantie de vitalité, et il faut y chercher les indications qui précisent les différentes évolutions possibles.

Pour ce qui est des décodeurs, le débat entre le microcalculateur détachable et le microcalculateur enterré est-il clos ? Je ne le pense pas en considérant les deux cas suivants.

— Parmi les évolutions suggérées pour Eurocipher, il y a un microcalculateur de sécurité détachable pour compléter l'action du microcalculateur de sécurité enterré afin de mieux contrôler l'expansion de la fraude.

— La voie choisie par Vidéocrypt comporte dès le départ deux microcalculateurs de sécurité : les droits d'accès figurent dans une carte, comme dans Eurocrypt ; mais le décodeur contient un autre dispositif qui authentifie la carte qui doit contenir une accréditation convenable.

NOTE — L'accréditation est une signature de l'identité de la carte par une technique à clé publique. La carte peut prouver qu'elle dispose de l'accréditation requise sans révéler sa valeur par des techniques dites «à apport nul de connaissance» (en anglais, 'zero-knowledge techniques'). Le vérificateur doit seulement utiliser la clé publique publiée par l'autorité qui délivre les accréditations.

L'usage simultané de deux microcalculateurs de sécurité, l'un enterré, l'autre détachable, permet certainement de mieux contrôler l'évolution de la fraude en compliquant la tâche des fraudeurs.

L'usage simultané de deux microcalculateurs de sécurité, l'un enterré, l'autre détachable, permet aussi à une autorité ayant fait développer et commercialiser des décodeurs d'en contrôler l'usage par des opérateurs, ce qui peut poser un certain nombre de problèmes éthiques et institutionnels.

Les techniques à apport nul de connaissance, stade ultime de l'évolution des techniques cryptographiques à clé publique, ont également un impact important sur l'évolution des cartes à puce elles mêmes.

Ainsi, des cartes peuvent à l'avenir être émises par un organisme (ou plusieurs organismes) reconnu et accepté par les gérants de services. Le rôle d'un tel organisme est d'homologuer et de labelliser les modèles de cartes proposés par les constructeurs, et d'harmoniser les travaux de normalisation et de spécification. Un tel organisme pourrait être un GIE européen, une Banque centrale, ...

Les cartes peuvent ensuite être vendue librement sous emballage scellé dans les magasins. Les usagers les acquièrent. Et à la passation d'un contrat entre l'usager et un gérant de services, une ou plusieurs entités dédiées sont créées dans la carte, par délégation de l'autorité ayant émis la carte.

SOME STUDIES ON A CONDITIONAL ACCESS SYSTEM FOR DBS TELEVISION SERVICE

ALGORITHMS OF PERMUTATION SCRAMBLING AND AN EXPERIMENTAL DECODER WITH SMART CARD

Takeshi **KIMURA**, Masafumi **SAITO**, Seiichi **NAMBA**
NHK - Japan Broadcasting Corporation
Science and Technical Research Laboratories
1-10-11 Kinuta, Setagaya-ku
TOKIO 157
JAPAN
Tél : +81 3 415 5111

ABSTRACT

Among the many scrambling techniques, line permutation is widely used. Here some typical algorithms of a line permutation scrambling method are described and compared. Also the idea of «depth-control» is introduced.

In a conditional access system, the security of the receiving end is very important. To realize a secure system, a smart card is applied to our experimental conditional access system. An outline and the features of the system are described.

RÉSUMÉ

La permutation de ligne est largement utilisée parmi les nombreuses techniques de brouillage. Certains algorithmes typiques de la méthode de brouillage de permutation sont décrites et comparées. Nous avons également introduit une idée de «contrôle de profondeur» («depth-control»).

Dans le système d'accès conditionnel, la sécurité de l'extrémité de réception est très importante. Pour réaliser un système sur, la carte à microprocesseur est appliquée à notre système d'accès conditionnel expérimental. Les particularités et données générales du système sont décrites.

TABLE OF CONTENTS

1. Introduction

We have been making various studies on a conditional access system, signal scrambling and access control techniques. And some of the studies have contributed to make up the technical standards of Japan. In this paper, we are going to present two subjects. One is the algorithms of line permutation scrambling methods, and the other is our experimental conditional access system adopting a smart card.

In recent years, the needs for a conditional access system are growing, along with the diversity of people's needs towards broadcast programs and an increase in broadcasting channels with the development of DBS and CATV. In Japan, against this background, the technical standards of a conditional access system for DBS pay TV was specified by ordinance in 1990. A broadcasting service based on these technical standards is going to be started in 1991 by JSB (Japan Satellite Broadcasting Corporation) via the BS-3a satellite. Also, the technical standards for a quasi-broadcasting service through communication satellite is now under study.

2. Line permutation algorithms and its characteristics

Many picture scrambling techniques have been developed. Among them, the line rotation scrambling technique and line permutation scrambling technique demonstrate good performance in the unrecognizability of scrambled pictures and provide security against unauthorized decoding. For that reason they are widely adopted in high security conditional access systems.

Line permutation scrambling is a technique that transmits the video signal after permuting the order of its original scanning lines. Suppose that the number of scanning lines per block in which the permutation executes is N, the number of all the possible permutation is N! (factorial of N). If N = 240 (approximate the active lines per field in the NTSC system), N! becomes an enormous number of $4.1*10^{468}$. This large amount of possible permutations is the reason that the line permutation scrambling provides good security. And for the same reason, there are many algorithms for line permutation scrambling. In this section we discuss line permutation scrambling algorithms.

2.1 Introduction of depth control

Preceding our main discussion of line permutation scrambling, we will introduce the idea of the "depth-control" of signal scrambling. Ordinarily, the scrambled signal is required not to be recognized by the original signal. This is very true in the case of telecommunication which is to be done between specially fixed stations. But, in the case of broadcasting, where programs are transmitted toward many general receivers, the broadcaster doesn't always intend that unauthorized

receivers not receive his program, but rather intends them to promote a contract with and receive his program. So, on special occasions, it is desired to reduce the unrecognizability of the scrambled signal to the degree that the subject of the program can be recognized but the program can not be enjoyed. In such circumstances, the idea of "depth-control," which means the conscious reduction of the unrecognizability of the scrambled signal based on these aims or the technique to achieve it, is very suitable for (perhaps only for) broadcasting.

Considering the "depth-control" technique, the following points are important:

(a) The service which the authorized receivers accept should not be impaired because of the addition of the depth-control function.
(b) The addition of the depth-control function does not increase the cost of the decoder nor the expense of the authorized receiver.
(c) The depth-control scrambled signal (picture or sound) should not be so unpleasant and be acceptable, if possible.

In the line rotation scrambling system, the degree of unintelligibility can easily be controlled by limiting the positions of the cut points. With the line permutation system, this is also possible, and the methods of achieving depth-control are taken into account in the following consideration of the line permutation algorithms.

2.2 Line permutation scrambling methods

Some typical methods and algorithms for line permutation scrambling are described in this section.

2.2.1 Shuffling table look-up method

The most easy and direct way to realize a line permutation scrambler or descrambler is to have a table that contains some shuffling maps. The original lines are put into memories in regular order and scrambled lines are accessed out of memories in the shuffled order the table addresses. Suppose that the table contains K-kinds of shuffling maps, there may be K permutations. So, the security of the system is limited by the size of the table, that is, usually by the size of the ROM.

Some modification can be made in this shuffling table method to improve the security. For example, the original lines are put into memories in the shuffled order the table addresses and scrambled lines are accessed out of memories again in the shuffled order. This system has K^2 permutations.

2.2.2 N! shuffling algorithm

The first scrambled line will be selected from N original lines, the second line will be selected from the other N-1 lines, and so on for be the 3rd through Nth line. All these selections will be N! ways. The N! shuffling algorithm executes the permutation in this manner.

Algorithm 1

(1) Repeat (2) and (3) while scanning I from 0 to N-1.
(2) Select J randomly between I and N-1.
(3) Exchange the Ith line and Jth line.

In step (2), J will be selected from a different range at every repetition. This may be achieved by the product of the range and a random source. Then, N times of product operation is necessary.

2.2.3 N^N shuffling algorithm

This algorithm is a modification of the previous algorithm.

Algorithm 2

(1) Repeat (2) and (3) while scanning I from 0 to N-1.
(2) Select J randomly between 0 and N-1.
(3) Exchange the Ith line and Jth line.

Modification is made in step (2). The range, in which J is selected, is fixed at every repetition. So, this algorithm enables faster operation in micro-processing.

This algorithm has N^N routes in the permutation result. But of course there are at most N! sets of the permutation result. Some subsets of the route cause the same permutation result.

In the N^N shuffling algorithm, depth control can be achieved by executing step (2) as follows.

Algorithm 2-1

(1) Repeat (2) and (3) while scanning I between 0 and N-1.
(2) Generate random number R in the range 0 and D-1.
(D is the index number of depth-control)
Let J = (I + R) modulo N.
(3) Exchange the Ith line and Jth line.

In these ways the distance of the two swapping lines in every step (3) is limited within D. So the scrambling depth can be controlled. For full scrambling let D = N, and for controlled scrambling let D be smaller. You can see in Fig.5-(3) that the scrambled line remains near the original line position, but the scrambled lines are not

equally distributed upward and downward.

In order that the controlled-depth scrambled lines are equally distributed upward and downward, scanning in step (1) needs to be in shuffled order. For example, it may be directed by a random scanning table, or more easily interleaved scanning may be available. An example of a scrambled picture by interleaved scanning is shown in Fig.5-(4).

2.2.4 Line number ciphering -1

A block diagram of a scrambler or descrambler using this method is shown in Fig.1. The original lines are put into memories in the regular order addressed by counter-1, and the scrambled lines are accessed out of memories in the ciphered order that is addressed by counter-2 and the cipher circuit.

In general, the x-bit cipher circuit enciphers 2^X members of plain text into 2^X members of cipher text. However, the number of lines N per block is not always just 2's power. Without checking the ciphered line number, a line number which exceeds N will be generated. To avoid this, a checking circuit must be added. And if the ciphered line number exceeds N, the checking circuit makes counter-2 count up again to regenerate a new line number.

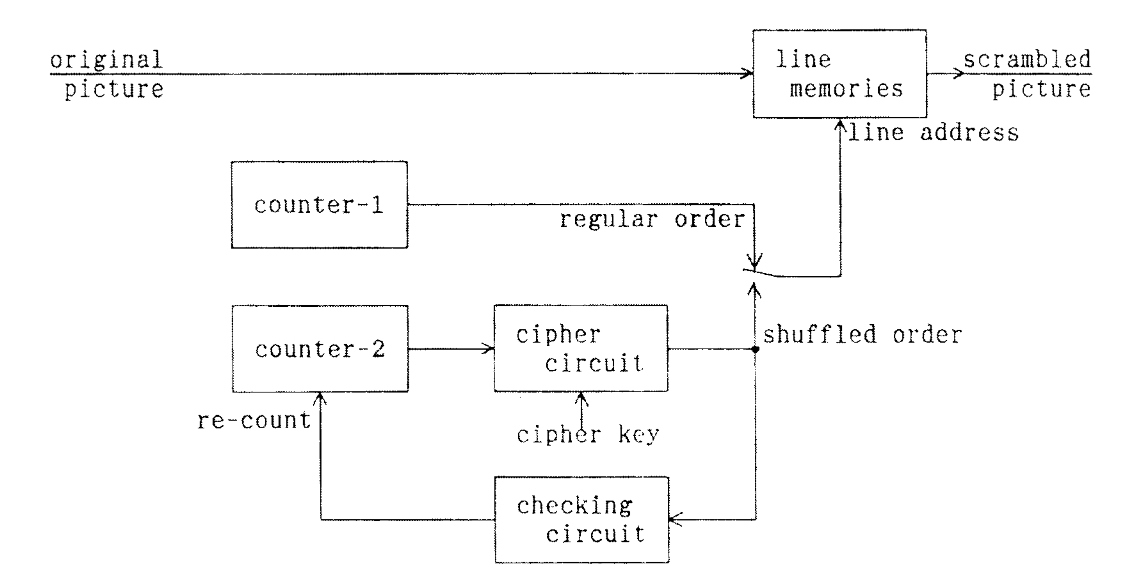


Fig.1 Line number ciphering -1

2.2.5 Line number ciphering -2

The principle of this method is similar to the previous line number ciphering -1. A block diagram of a scrambler or descrambler using this method is shown in Fig.2. The difference is the N member cipher circuit, which ciphers N members of plain text into N members

of cipher text. This method can save the test circuit and the counter-2, and also save address regeneration time.

An example of this type of cipher circuit is shown in Fig.3. Suppose that N is a product of two integers N1 and N2. Then, one of the N members can be expressed by the two components x and y, either of which is a member of N1 or N2 respectively. First, x0 is mapped into x1, with the mapping a function of y0 and the cipher key. Then, y0 is mapped into y1, with the mapping a function of x1 and the cipher key. These stages are repeated several times. In each stage, mapping can be realized by modulo N1 addition, small mapping tables, or a combination of these.

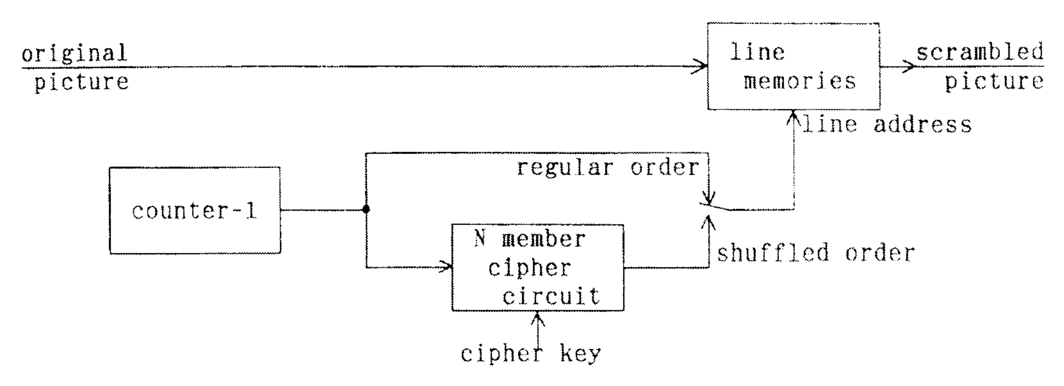


Fig.2 Line number ciphering -2

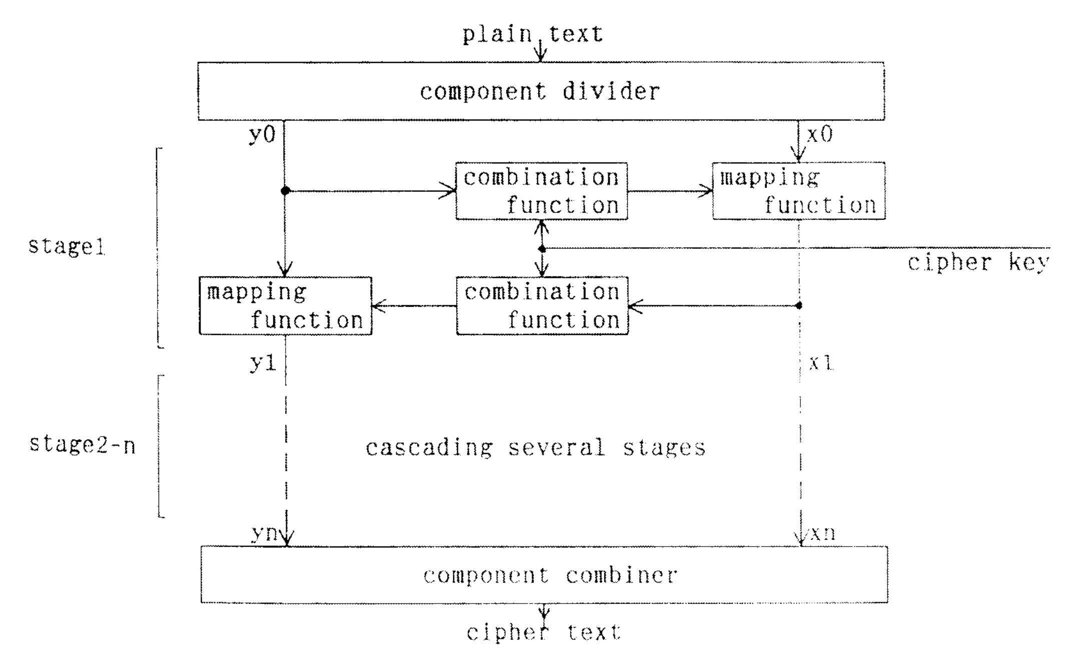


Fig.3 An example of N-member cipher circuit

The depth control can be achieved by bypassing all the mapping of component x, while x is the most significant component. In this case, the scrambled picture will be divided into N1 sub-blocks of N2 lines as in Fig.5-(5).

2.2.6 Memory address control method (Non-block line permutation)

All the methods described above require a memory capacity of at least N lines in the scrambler and descrambler. On the other hand, the following method can realize a descrambler with less memory capacity than N lines without sub-blocking. Suppose that the memory capacity is selected to be M lines, the descrambling algorithm is as follows:

Algorithm 3

(1) Repeat (2) while scanning I between 0 and M-1.
(2) Put scrambled line into Ith memory.
(3) Repeat (4) and (5) (N-M) times.
(4) Select I between 1 and M randomly.
(5) Access descrambled line out of Ith memory, and put scrambled line into Ith memory.
(6) Repeat (7) while scanning I between 0 and M-1.
(7) Access descrambled line out of Ith memory.

In (1) and (2), the first M scrambled lines are stored in the line memories. Next, in (3),(4) and (5), a descrambled line is access out of a line memory, and at the same time a scrambled line replaces that space in the memory. This operation is repeated until the last scrambled line is put into the memory. And just after this, the memory contents the last M lines. Then, in (6) and (7), the last M descrambled lines left are swept out of the memory, and the descramble operation in a block of N lines completes.

According to this algorithm, the descrambler requires a memory capacity of only M lines, while the permutation block is N lines. But the memory of the scrambler that executes the inverse permutation needs to have a capacity of N lines.

2.3 Comparison of permutation methods

Some examples of the scrambled picture are shown Fig.5. A comparison of these permutation methods is shown in Table 1. In this table, the comparison is done for the following items:

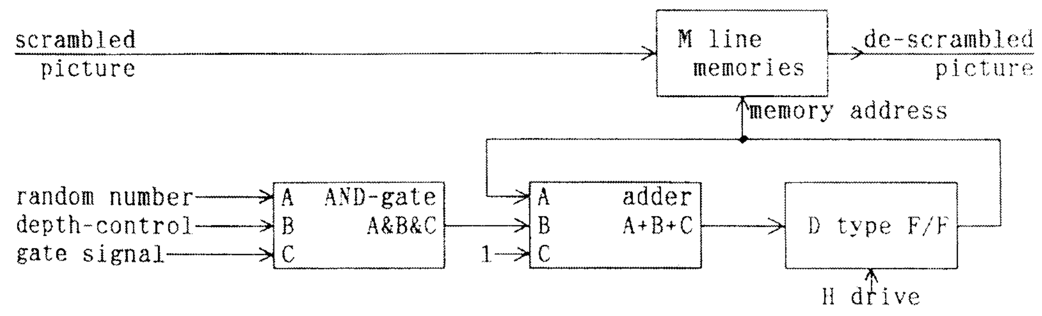
(a) the number of possible permutations
(b) the mode of the random number: line-by-line random sequences or random key per block
(c) hardware necessary to build the descrambler: memories for the picture signal, and a controller to manage the permutation

(d) necessity of software
(e) depth-control

2.4 Method adopted in Japanese DBS pay TV [1]

In the transmission standards of (NTSC) pay television broadcasting via satellite in Japan, the memory address control method (the non-block line permutation method in its term) is used as the method of line permutation, because of the simplicity of the control circuits. The transmission standard is specified by calculation of the inverse permutation, according to the descrambler algorithm. The following is an outline of the system.

Scrambling lines ---- 240 lines (23H - 262H, 286H - 525H)
Scrambling memories -64 lines
Depth-control ------- 3 degrees
(full / color periodical / 32-line periodical)
Descrambler circuit - Fig.4



random number - 6 bits of line-by-line random sequences
depth-control - full .... 111111(binary)
color periodical 111110
32 line periodical .. 100000
gate signal---- 86H-262H, 349H-525H . 111111
other lines 000000

Fig.4 A memory address control method in the Japanese system

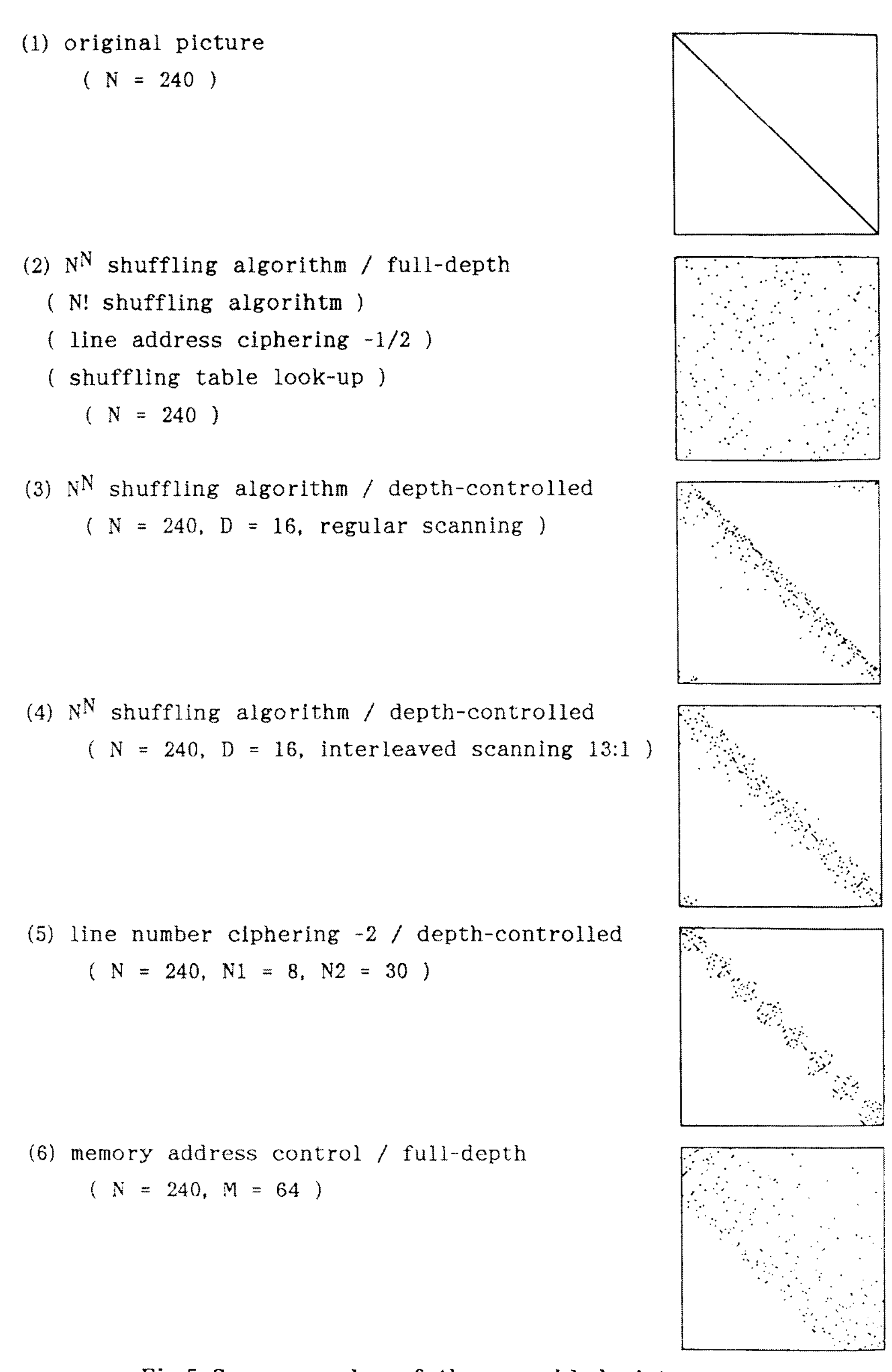


Fig.5 Some examples of the scrambled picture

method	number of permutations	mode of random number	hardware		software	depth-control
			picture memories	memory controller		
table look-up	K or K^2 K:maps/table	block key	N or 2N lines	counter table	none	
N! algorithm	N!	line-by-line sequences	N or 2N lines	micro-processor	N product operations	
N^N algorithm	N!	line-by-line sequences	N or 2N lines	micro-processor	more simple than N!	see 2.2.3
line number ciphering-1	2^K K:bits/key	block key	N or 2N lines	2 counters cipher circuit check circuit	none	
line number ciphering-2	2^K K:bits/key	block key	N or 2N lines	counter cipher circuit	none	see 2.2.5
memory address control	$M^{(N-M)}$	line-by-line sequences	M lines	very simple (see fig.5)	none	see 2.4 & fig.5
(scrambling part)			N or 2N lines	micro-processor	simulate descrambler	

Table1 A comparison of the line permutation methods

3. Experimental conditional access system

The experimental equipment of the conditional access system is shown in this section. Using this equipment, a Japanese DBS conditional access broadcasting system and other picture scrambling techniques, including some of the line permutation scrambling methods described in this paper, sound scrambling techniques and access control techniques are examined.

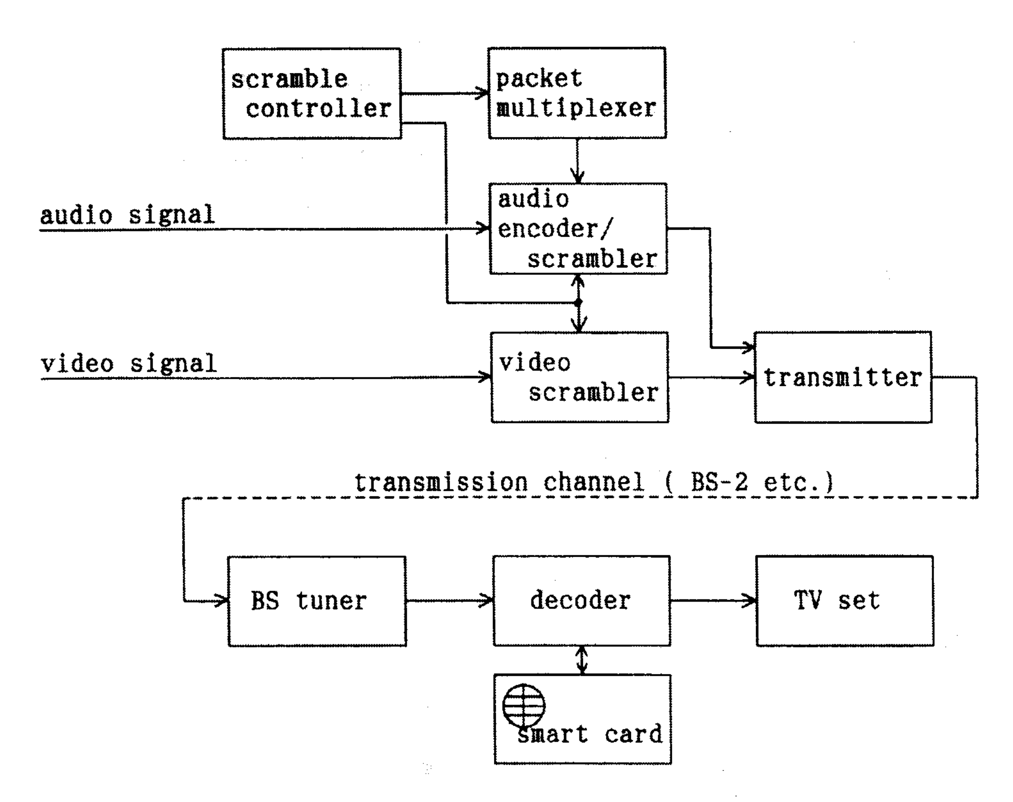


Fig.6 Outline of the experimental conditional access system

3.1 Outline of a conditional access system for DBS in Japan [1]

This system is applied to the digital sub-carrier/NTSC system.

The methods of picture scrambling are line rotation or/and line permutation, and they are controlled by a pseudo-random sequence generator.

The method of sound scrambling is exclusive-OR combination bit by bit of the sound data (except for range bits) with the bits of a continuously running pseudo-random generator.

Pseudo-random sequence is generated by non-linear combinations of the outputs of three multistage linear feedback shift registers (13, 11 and 8 stages each), and the timing signal is transmitted as a part of the sound frame control codes.

Four types of access control messages are available as messages necessary for descrambling at the receiving end and for controlling the

pay television service.

(a) the "program related message", which includes
 - a key for descrambling picture and sound
 - bits for expressing subscriber groups who have program access entitlement
 - the price of the program, etc.

(b) the "descramble direct control data", which disables the descrambling function of stolen or unauthorized receivers forcibly, or restores the descrambling function.

(c) the "individual subscriber's message", which includes
 - an authorization key to decipher the program related message
 - subscriber contract data, etc.
   (Many types of subscription contract, such as flat fee, tiered and pay-per-view, are available.)

(d) the "Message data for display", which conveys the information concerning the pay TV service.

Program related messages, descrambler direct control data, and message data for display are transmitted in a packet format on the data channel, which is the free area in the digital sound signal transmission format. The length of the packet is 288 bits. Individual subscriber's messages are distributed on the data channel, or using physical media.

3.2 Experimental transmitting equipment

The picture scrambler can realize line rotation scrambling, line permutation scrambling and both at the same time. It has memories capable of two fields and one microprocessor. The microprocessor manages the memories for executing picture scrambling. Although there are some methods suitable for full hardware realization, as described in section 2, with this equipment, all the methods are realized by software to generalize the hardware.

The scramble controller consists of one personal computer. It sends the scrambling keys to the picture scrambler and the sound scrambler and transmits corresponding access control messages through the packet multiplexer, about every second. It also manages receivers' information and transmits receivers' personal messages at the same time.

3.3 Equipment at the receiving end [2]

We adopted a smart card system in the access control part of our experimental equipment. The functions which the decoder and the smart card take respectively are shown in Fig.7.

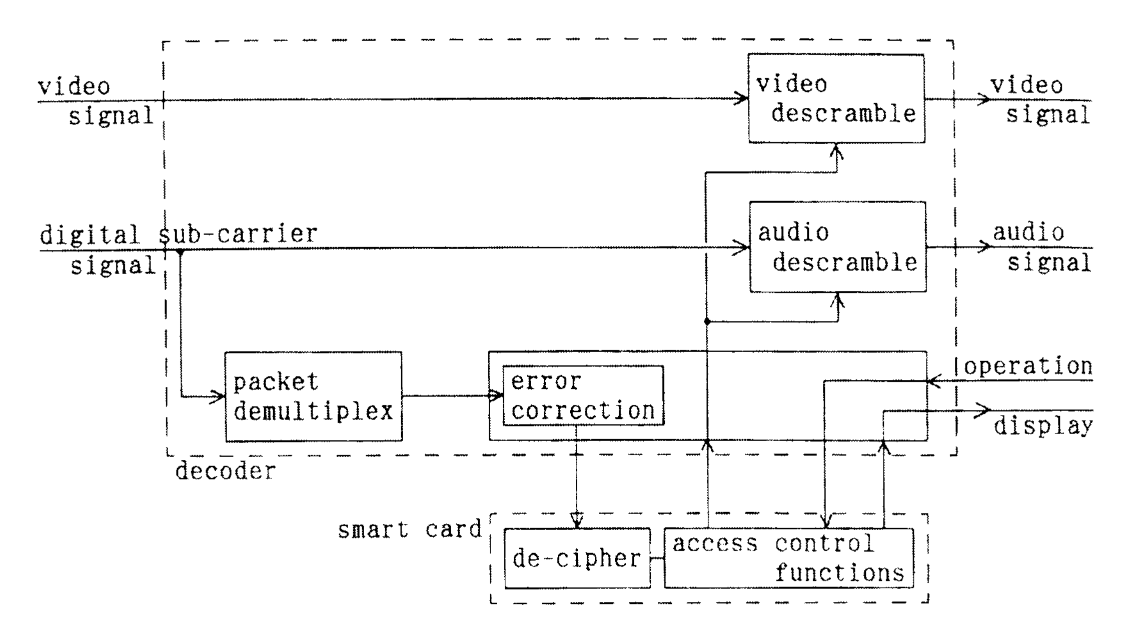


Fig.7 Functions in the decoder

3.3.1 Decoder

The functions that the access control part of the decoder takes are:

(a) descrambles the picture signal
(b) descrambles the sound signal
(c) de-multiplexes the access control message packet from the digital sub-carrier
(d) corrects errors in the access control message packet
(e) sends the access control message packet to the smart card
(f) receives the descrambling key in response, and gives it to the descrambling part
(g) inputs the audience operation (request to view, etc.), and reports to the smart card
(h) receives the message (program price, etc.) from the smart card, and displays it.

The picture descrambler and the sound descrambler execute functions (a) and (b), respectively, and the packet de-multiplexer executes function (c). These are built in as exclusive-use hardware.

A general purpose 8-bit microprocessor executes functions (d)-(h), while it has peripheral hardware for the error correction. These functions are mostly interfaces between the descrambler, the audience and the smart card.

3.3.2 Smart card

The smart card used in this equipment is based on the ISO

standard. It has a mask ROM for instructions and also an EEPROM for instructions and data.

All of the access control messages mentioned in 3.1 are processed in this smart card. And the functions that the smart card executes are:

(a) deciphers the access control messages
(b) manages access control:
 - checks if access to the program is permitted
 - manages fees
 - keeps information about the contract
(c) manages some parts of human interfaces:
 - inputs and interprets operation
 - outputs display messages
(d) keeps information about the program viewed

Functions (a) and (b) are those of security, and (c) and (d) are additional ones.

These security and human interface functions which the smart card executes can be updated by replacing the smart card, if this is necessary. And in this smart card, the functions can be updated also by the broadcaster's terminals or over-air because the instruction codes may be allocated on the EEPROM area.

The interface signals that connect the decoder and the smart card are:

(a) the access control message packet
(b) the descramble key
(c) information about audience operation
(d) the display message

3.4 Features of the smart card system

The smart card system has the following features:

(a) The smart card is separated from the decoder.
(b) The decoder has no secrets.
(c) The decoder need not be personalized.
(d) Almost all of the security part is in the smart card.
(e) The smart card can be personalized, if necessary.
(f) The instruction codes for the security functions may be allocated in the EEPROM area.

Also, it gives some benefits to each person. Of course, supposing that the smart card remains in the decoder, it provides the same benefits as s system without a smart card. Further benefits are:

(a) For the manufacturer...
 - Decoder manufacturers are freed from keeping secrets and electrical

numbering, so that they can manufacture and distribute the decoders similarly to other goods.

- Also, smart card manufacturers are freed from keeping secrets, because the instruction codes can be stored in the card at the user (broadcaster) end.

(b) For the broadcaster...

- The broadcaster need supervise only the smart cards, which are small and easy to handle.
- Also, it is difficult to access the secrets by breaking the smart card; more difficult than in the case of a mask ROM.
- The broadcaster can adopt his own private security functions, by providing his customers with his exclusive smart cards.
- And even if his secret is let out, new security functions can be adopted by providing a new smart card.

(c) For the authorized receiver...

- He can choose his favorite decoder model independent of the broadcaster with whom he has contracted.
- Those who possess a smart card can enjoy programs with any decoder.

References

[1] "Technical standards on a conditional-access broadcasting system for application to satellite television", Report of Telecommunications Technology Council for Ministry of Posts and Telecommunications, 1988 (in Japanese).

[2] M.Saito, T.Kimura, S.Namba: "A study on an Application of IC Cards in a Broadcasting Receiver", Nat. Conv. IEICE(Spring), B-198, 1989 (in Japanese)

UN SYSTÈME D'ACCÈS CONDITIONNEL
POUR LES RÉSEAUX DE DIFFUSION LARGE BANDE
EUROCRYPT

Françoise **COUTROT**, Vincent **LENOIR**
CCETT
4 rue du Clos Courtel - BP 59
35512 CESSON SEVIGNE Cedex
FRANCE
Tel : +33 99 02 41 11

RÉSUMÉ

Le système EUROCRYPT vise le marché de la TV payante sur satellite de diffusion directe, les réseaux câblés ou les réseaux hertziens. La sécurité du système repose sur l'usage de cartes à mémoire. Il permet une approche ergonomique et conviviale des services de TV payante. Ce système, prévu pour une gestion multi-services des opérateurs, est également évolutif. Aujourd'hui, Eurocrypt a été retenu par le CSA en France pour les chaînes payantes sur TDF1/TDF2, par FRANCE TELECOM pour les services payants de ses réseaux câblés et, en Scandinavie, par Scansat pour la communication de ses programmes ASTRA.

ABSTRACT

The Eurocrypt system is aimed at the DBS, CATV and terrestrial pay-TV services. Security of the system relies on smart card use. It allows an ergonomical and userfriendly approach of pay-TV services. This system includes multi programme provider management and evolutivity facilities. Nowadays, Eurocrypt has been chosen by CSA in France for pay-TV channels of TDF1/TDF2, by FRANCE TELECOM for pay-TV services on its cable networks and, in Scandinavia, by Scansat for its ASTRA programmes.

TABLE DES MATIÈRES

UN SYSTEME D'ACCES CONDITIONNEL

POUR LES RESEAUX DE DIFFUSION LARGE BANDE

EUROCRYPT

Françoise Coutrot et Vincent Lenoir (C.C.E.T.T.)

L'accroissement considérable des capacités techniques de diffusion apporté par le câble et les satellites conduit des opérateurs de plus en plus nombreux à proposer des programmes dont le financement traditionnel (par les redevances ou la publicité), est devenu insuffisant et doit être complété par des moyens de financement direct par les usagers sous la forme d'abonnements ou de paiement à la consommation. Cette approche commerciale est par ailleurs confortée par l'évolution des modes d'achat de l'usager vers un mode de consommation "à la demande".

La mise en service de ces nouveaux supports de diffusion s'est concrétisée par le lancement de satellites de diffusion directe dès fin 1988 et la progression constante du nombre de prises câblées jusque chez les abonnés s'accroît tant en France que dans les autres pays européens (Allemagne, Belgique...). Sur l'ensemble de ces réseaux, opérateurs de services (et, derrière eux, les industriels) sont très motivés pour fournir un service de TV payante.

Cette convergence dans le besoin exprimé a conduit FRANCE TELECOM, et au travers de ses laboratoires, le CCETT, à définir un système d'accès conditionnel qui permette de couvrir les besoins en matière de TV payante de façon **unique**. Cette unicité de définition est en effet indispensable si l'on veut mettre en commun un certain nombre d'équipements d'investissement lourd (tels que les centres de gestion des usagers) et présenter à l'usager un accès technique relativement uniformisé. Cette gageure devait être tenue malgré la diversité des réseaux, des types de signaux transportés et des techniques d'embrouillage utilisées.

Les résultats de cette étude menée au CCETT sont rassemblés dans le système d'accès conditionnel **EUROCRYPT** dont une première réalisation utilise la carte à mémoire PC2.

1. Techniques d'accès conditionnel

Les techniques de TV payante reposent sur deux mécanismes indépendants ; d'un coté, l'embrouillage de l'image et du son et de l'autre la gestion de droits d'accès commerciaux qui doivent être traduits sous forme de messages sécurisés vers les terminaux. Dans le cadre de l'étude Eurocrypt nous ne nous sommes intéressés qu'au second aspect de la technique. Il suffit, en effet, pour adapter le système Eurocrypt aux techniques d'embrouillage de connaître les caractéristiques des signaux transmis, de synchronisation et d'identification sur les différentes chaînes. L'interface entre "embrouillage" et "accès conditionnel" se matérialise par un **mot de contrôle** qui permet de synchroniser et d'initialiser de la même façon l'embrouilleur du transmetteur et les désembrouilleurs des récepteurs autorisés.

Les messages d'accès conditionnel sont de deux types :
- les **messages de contrôle des titres d'accès** qui sont associés, en temps réel, à la transmission du programme. Ils transmettent une forme chiffrée des mots de contrôle. Ils incluent également les critères d'accès au programme : numéro de l'émission, coût de l'émission, niveau du programme... ; ces critères sont appelés paramètres d'accès. Ces données sont transmises au processeur de sécurité (présent dans une carte à mémoire). Celui-ci délivre, en retour, le mot de contrôle au désembrouilleur, **à la condition** qu'un des droits d'accès de l'usager mémorisés dans le processeur couvre les paramètres nécessaires à l'accès du programme. Les mots de contrôle sont renouvelés toutes les 10 secondes environ (dissuadant ainsi une commercialisation frauduleuse de ces derniers). Les messages de contrôle des titres d'accès transmettent la forme chiffrée du mot de contrôle courant et du suivant de façon à permettre l'anticipation du calcul par le processeur de sécurité.
- les **messages de gestion des titres d'accès** qui transmettent les nouveaux droits aux terminaux des usagers (renouvellement d'abonnement, numéros des programmes,...). Les droits ainsi émis sont mémorisés dans le(s) processeur(s) de sécurité concernés par l'autorisation. Sous ce type de messages sont également compris les messages nécessaires à la remontée des consommations. La carte à mémoire vérifie, avant de communiquer les données relatives au relevé de consommation, qu'elle a l'opérateur autorisé en face d'elle, ceci en effectuant une authentification de l'opérateur de service. En fin de relevé, l'opérateur inscrit de façon sécurisée une butée dans la carte de façon à marquer la fin du relevé. Ces messages peuvent être transmis de façon différée à l'usager et sur un réseau différent de celui supportant la transmission du programme.

Les deux types de messages, contrôle ou gestion, sont sécurisés contre toute modification de leur contenu.

2. Modes de commercialisation des services de TV payante

Les modes de commercialisation sont de deux types différents :
- abonnement par thème, niveau ou classe : ce mode permet de vendre aux usagers un programme pour une période donnée en diversifiant l'offre par thème (sports, musique...) ou par niveau (du plus basique (par exemple, film en rediffusion) au plus complet (film en rediffusion et en exclusivité)).
- paiement à la séance : ce mode permet à l'opérateur de vendre son programme à l'évènement. L'usager peut acheter son titre à l'avance : il appelle alors le centre de gestion et reçoit en retour son droit : c'est l'achat anticipé. L'achat peut également être "impulsif" auquel cas l'usager peut acheter l'émission sur décision locale moyennant le débit dans sa carte d'une zone de crédit pour le prix correspondant à l'émission. Dans ce dernier cas, l'usager peut acheter l'émission au forfait ou à la durée.

L'achat impulsif pose un problème particulier lié au choix local des émissions par l'usager. En effet, le centre de gestion ne connaît plus les choix effectués par les usagers contrairement aux autres modes de commercialisation ; il n'a donc pas les éléments nécessaires à l'audimétrie des programmes et au paiement des ayant-droits. Pour assurer cette remontée des consommations, il faut prévoir une voie de retour vers le centre de gestion. Les terminaux fonctionnant en achat impulsif sont ainsi munis d'un modem connecté sur le réseau téléphonique. Cette fonction permet également de faire une facturation a posteriori des usagers en fonction des émissions regardées (facturation détaillée).

Un même programme ou évènement peut être accessible suivant un ou plusieurs des modes de commercialisation décrits ci-desssus et ceci sur choix

de l'opérateur. Il suffit alors de reporter les paramètres idoines dans les messages de contrôle des titres d'accès.

En plus des modes de commercialisation à proprement parler, le système offre des fonctions complémentaires telles :
- l'occultation de zones géographiques : cette fonction n'est nécessaire que sur les réseaux satellites (à très large couverture géographique) et permet d'occulter un ou plusieurs pays pour un programme dont les droits de commercialisation n'auraient pas été acquis par l'opérateur.
- l'envoi de messages personnalisés à l'attention d'usagers ou de groupes d'usagers.
- la pré-sélection de programmes par l'usager : cette fonction permet à l'usager de pré-valider des émissions qui seront diffusées en son absence (par exemple des émissions à achat impulsif). Cette fonction est particulièrement utile pour permettre l'enregistrement de programmes désembrouillés sur magnétoscopes en l'absence de l'usager.
- un contrôle local de l'usager qui lui permet de verrouiller l'usage de sa carte et de conditionner son utilisation à la présentation d'un code parental. Ce verrouillage peut s'appliquer à la validation lors de l'achat impulsif ou à la pré-sélection de programmes.

3. Organisation du système

Le système Eurocrypt a été conçu pour permettre, avec le minimum de contraintes de coopération pour les opérateurs de service, un partage du système, voire de la ressource carte à mémoire.

Ceci est possible par la hiérarchisation des fonctions de gestion des cartes à mémoire. L'initialisation et la mise en service des cartes est réalisée par l'**autorité émettrice** qui est garante de la sécurité du système. Cette autorité est responsable de l'ouverture ou de la fermeture de zones de service allouées aux opérateurs de service. Une fois la zone de service ouverte, chaque **opérateur de service** gère de façon indépendante et autonome la ressource qui lui est affectée. Le système est conçu de telle sorte qu'aucune interaction n'est possible entre opérateurs de service, ceci par la définition de secrets propres à chacun.

La mise en place du service auprès des usagers suppose la fourniture de terminaux et de cartes. Les terminaux peuvent être achetés par l'usager sur le marché libre ou loués par des opérateurs de service eux-mêmes propriétaires des équipements. Les cartes sont achetées par les opérateurs de service qui les distribuent aux usagers ; les cartes restent la propriété, in fine, des opérateurs de service.

4. Sécurité du système

Cette sécurité est réalisée à deux niveaux :
- la mise en oeuvre d'un **processeur de sécurité performant** : la carte à mémoire PC2 qui contient les clés secrètes des services (clés d'exploitation et de gestion) ainsi que les droits d'accès acquis par le télespectateur. Outre les aspects liés à la sécurité, l'utilisation d'une carte à mémoire présente l'avantage que les désembrouilleurs, qui constituent l'investissement lourd du système, peuvent être banalisés et, le moment venu, être intégrés dans le téléviseur.
- une redondance sur les messages d'accès conditionnel, appelée **signature du message**, qui garantit l'intégrité de ces messages.

5. Adressage sur antenne

Une des caractéristiques du système EUROCRYPT est de permettre l'envoi des messages de gestion par le réseau de diffusion du programme. Ceci implique que les messages de gestion utilisent une partie de la ressource de données disponibles sur le signal. Cette fonction n'est concevable, au regard des audiences concernées (plusieurs millions de télespectateurs) que si le système offre une facilité de regroupement des usagers qui permette de s'adresser à l'ensemble de l'audience sur un temps de cycle très court. Cette facilité offerte par le système Eurocrypt permet de réduire le temps de cycle nécessaire à l'adressage de 1 million d'usagers de 1 heure (dans le cas d'adressage individuel) à 10 secondes (dans le cas d'adressage groupé). La technique utilisée est de regrouper les usagers par entités de 256 et d'émettre les droits communs aux usagers par adressage groupé. Les groupes peuvent être reconfigurés quand leur homogénéité (donc leur efficacité) décroît.

6. Evolutivité du système

Les messages d'accès conditionnel sont en "format libre" pour permettre une évolution des fonctionnalités et des algorithmes de sécurité du système. Il est ainsi possible d'introduire ultérieurement de nouveaux paramètres correspondant à de nouvelles fonctionnalités tout en garantissant une compatibilité ascendante du système et en garantissant le maintien de la sécurité. Il est également possible de changer d'algorithme ou la longueur des clés secrètes sans modifier les désembrouilleurs ; le processeur de sécurité étant détachable, il suffit en effet de changer les cartes à mémoire dans ce cas.

7. VISIOPASS : le service d'accès conditionnel offert par FRANCE TELECOM

FRANCE TELECOM a passé commande aux industriels des différents équipements entrant dans la chaîne d'accès conditionnel du système EUROCRYPT :

- des codeurs D2-MAC/PAQUET à accès conditionnel pour têtes de réseaux cablés ou points d'émission satellite : MATRA COMMUNICATION,
- des récepteurs : 750 000 équipements commandés à RPIC pour une réception câble et satellite,
- un centre de gestion des usagers et des cartes : une première version à SEMA GROUP et la version finale à TELESYSTEMES,
- les cartes à mémoire PC2 : BULL CP8.

La validation technique de l'ensemble du système est prévue pour juin 1990 permettant ensuite l'ouverture commerciale du service VISIOPASS.

CONCLUSION

Les choix qui ont participé à la définition et à l'implémentation du système EUROCRYPT permettent une simplification de la gestion des usagers et permettent aussi un partage de ressources communes entre opérateurs. Ce système est applicable à la fois sur les réseaux satellites et les réseaux câblés, accroissant ainsi son marché potentiel. Aujourd'hui, le système EUROCRYPT a été choisi par le CSA en France pour les services de TV payante sur TDF1/TDF2, par FRANCE TELECOM pour les services de TV payante sur ses réseaux câblés et, en Scandinavie, par SCANSAT pour la commercialisation de ses programmes sur ASTRA.

CONTRIBUTION À L'HISTORIQUE DU DÉVELOPPEMENT DES TECHNIQUES, NORMES ET TECHNOLOGIES DU SERVICES DE TÉLÉVISION À ACCÈS CONDITIONNEL EN VUE DE LEUR MISE EN ŒUVRE DANS LE SYSTÈME MAC PAQUET

Yves **GUINET**
La Radiotechnique Portenseigne
51 rue Carnot
BP 301
92156 SURESNES Cedex
FRANCE
Tel : +33 (1) 47 28 51 00

RÉSUMÉ

L'auteur examine l'introduction et le développement des fonctions télématiques, telle notamment celle de l'accès conditionnel, dans l'architecture du système audiovisuel domestique. Il analyse les modifications du comportement qu'elles induisent, tant au niveau du fournisseur de services audiovisuels, qu'à celui de l'usager de ces services.

CONTRIBUTION A L'HISTORIQUE DU DEVELOPPEMENT DES TECHNIQUES, NORMES ET TECHNOLOGIES DU SERVICE DE TELEVISION A ACCES CONDITIONNEL, EN VUE DE LEUR MISE EN OEUVRE DANS LE SYSTEME MAC PAQUET.

par Yves GUINET

INTRODUCTION

PREMIERE PARTIE

Les travaux et recherches de base menés en France, de 1975 à 1982.

DEUXIEME PARTIE

La spécification et le développement de la fonction "accès conditionnel" du système Mac Paquet (1983 - 1990)

A. La première phase de normalisation et de développement : le rôle de l'UER durant la période 1982 / 1984 - le contexte français
   1. le contexte de la création du groupe d'experts V/CA ;
   2. les travaux du groupe d'experts V/CA en 83/84.

B. le gel des travaux normatifs durant la période 84/87.

C. La seconde phase de normalisationn et de développement durant la période 87/90 - Mac Eurocrypt et Mac Eurocypher.

CONCLUSIONS

CONTRIBUTION A L'HISTORIQUE DU DEVELOPPEMENT

DES TECHNIQUES, NORMES ET TECHNOLOGIES

DU SERVICE DE TELEVISION A ACCES CONDITIONNEL,

EN VUE DE LEUR MISE EN OEUVRE DANS LE SYSTEME MAC PAQUET.

par Yves GUINET

Dans cet exposé, on retrace un historique des travaux de recherche, de développement et de normalisation des techniques et technologies de l'accès conditionnel en radiodiffusion tels que nous les avons vécus en France.

L'auteur souhaite montrer, sur la base d'exemples vécus, les contraintes auxquelles se trouve soumis le développement des nouvelles technologies de média audiovisuel.

Pour normaliser ces nouveaux systèmes, il faut d'abord acquérir des connaissances fondamentales sur une base partagée et suffisamment répartie. Puis il faut susciter une convergence des plans d'affaires des divers acteurs économiques concernés. Cette convergence des plans d'affaires n'est elle même que la manifestation d'un certain état favorable du milieu au sein duquel se développe la technologie de media et agissent les acteurs.

Il faut que ce milieu comprenne les potentialités nouvelles de ces technologies, qui ne s'expriment initialement qu'au travers d'un discours généralement hermétique.
La manifestation flagrante de ces potentialités n'apparait au milieu que par la réalisation de systèmes opérables suffisamment représentatifs.

L'accès conditionnel, qui constitue un perfectionnement de la session de communication audiovisuelle, est moins immédiatement compréhensible par le milieu que le perfectionnement de la présentation audiovisuelle (par exemple le nouveau format de l'écran ou la haute définition de l'image). Il concerne, en effet, les comportements humains et sociaux de communication.
La représentation imaginaire de ces comportements futurs est difficile, voire impossible in abstracto, pour celui qui n'y accède pas par une induction intérieure à sa propre culture scientifique et technique ;

En outre, l'introduction de ces comportements nouveaux dans le milieu impose une modification du cadre juridique qui codifiait les comportements antérieurs. Elle appelle donc, par nature, une certaine intervention d'un pouvoir en charge d'organiser la communication dans la cité.

Enfin, dans le domaine technique, l'accès conditionnel met en oeuvre les sciences et technologies nouvelles de la télématique. Il suppose donc un élargissement notoire de la culture technique traditionnelle de ceux qui dans les divers secteurs de l'économie audiovisuelle, réseaux, services, industries de produits finis ou semi finis, gèrent le développement de la technologie de média audiovisuel.

Cette propagation des concepts nouveaux dans le milieu peut se heurter à des résistances fortes, pour des raisons multiples, ou bien, au contraire, trouvant un terrain favorable, le pénétrer rapidement.

On distinguera deux parties dans cet exposé :

* celle des travaux et recherches de base qui furent menés de 1974 à 1982,
* et celle des activités de développement de la normalisation destinés à spécifier et à réaliser le nouveau média satellitaire audiovisuel, et qui durèrent de 1983 à 1990.

Dans un si long processus, le nombre des acteurs ayant contribué d'une manière importante, voire déterminante, est évidemment considérable. C'est pourquoi cet exposé ne doit être considéré que comme une simple contribution reflétant un vécu particulier, et qu'il faudrait compléter par beaucoup d'autres.

L'auteur s'est livré à l'exercice dans le but principal d'exposer pourquoi et comment le milieu socio-économique interagit avec le process d'innovation et de gestion de la technologie de média.

PREMIERE PARTIE

LES TRAVAUX ET RECHERCHES DE BASE MENES EN FRANCE DE 1975 A 1982

1. *Les travaux de recherche et développement menés en France sur les techniques et technologies de l'accès conditionnel au média audiovisuel trouvent leur point de départ dans la création du CCETT, en 1972, du fait du rapprochement des cultures audiovisuelles et des cultures télé-informatiques que ce rapprochement induit (le rapport NORA - MINC n'a pas encore promu le concept de "télématique").*

   Les nouveaux programmes de recherche mis en place au CCETT, en 1973/74 comportent par exemple :
   * *le système Didon de diffusion de données par paquets dans un canal de télévision,*
   * *le système de videographie Antiope,*
   * *le système de télémessagerie Epéos,*
   * *le système de télévision à accès conditionel Discret.*

   Des articles, publiés dans le numéro 40 de la Revue de Radiodiffusion Télévision, dès 1975 décrivent leur nature et leur contexte socio-économique d'alors (Ref. 1).

   Le système Discret trouvera d'abord quelques applications professionnelles (émissions médicales, émissions éducatives) mais son prolongement principal interviendra en 1982 avec la mise en place du service de Canal Plus en VHF.
   Une technique d'embrouillage de l'image, expérimentée avec Discret, sera retenue.
   Le système de gestion de l'accès retiendra une technique simple, à secret enterré (les technologies de type Didon / carte à mémoire ne sont pas encore suffisamment matures pour être utilisées).

   En fait, les travaux initiaux de R&D, relatifs à la gestion de l'accès, seront surtout portés par le service télématique de vidéographie diffusée et les services de diffusion de données à accès conditionnel. On observera une situation comparable au Royaume Uni.

2. *C'est dans le courant de 1978 que le Directeur Général de TDF (Monsieur REMY), et son Directeur Technique (Monsieur BUFFARD), stimulent activement la reflexion prospective des Centres de recherche de TDF sur les systèmes de radio-diffusion à condition d'accès, l'organisation et la gestion de la messagerie d'accès.*

C'est dès cette époque que se dégage l'importance fondamentale technique, mais surtout économique et juridique, du concept de système à secret détachable.

Deux programmes de recherche et développement sont mis en place par TDF :

* l'un (confié à G. BERNEDE et J. GREGEOIS), aux Laboratoires d'Issy les Moulineaux, développe un système utilisant la carte à pistes magnétiques et le secret enterré.
  Ses résultats sont décrits dans l'étude 5312A de mars 1980 (Ref. 2).
* l'autre (confié à L. GUILLOU), aux Laboratoires du CCETT, développe un système utilisant la carte à micro-processeur.

Un premier marché d'études pour cette application de la "carte à mémoire" est passé à CII HB, à la fin de 1979. Quoique l'application d'affaires immédiatement visée soit, comme déjà indiqué, le service de vidéographie diffusée (Didon / Antiope) à péage, le rapport de présentation à la Commission des marchés précise bien "que les principes et technologies ... peuvent être étendus à tout système de radiodiffusion comportant une voie numérique de signalisation".

Ce sont les travaux menés dans le cadre de ces deux programmes de R&D qui permettront de dégager progressivement les principes fondamentaux et l'architecture des systèmes.

La Direction des Etudes et Recherches de TDF édite, le 6 Octobre 1982 le document intitulé "Addendum à la Spécification Didon - Antiope pour le contrôle d'accès" (LAR/CAS/100/82/LG). Il a été préparé par Louis GUILLOU et est représentatif de l'état de l'art à cette époque (Ref. 3) :
"La messagerie d'accès et les données chiffrées sont reçues par le terminal. La messagerie d'accès les délivre à un "porte clé" détachable du terminal où elle est traitée pour fournir au terminal "la combinaison d'accès".

La messagerie d'accès est constituée d'instructions de validation comprenant :

* un identificateur d'audience qui en définit les destinataires,
* un paramètre de validation qui définit les conditions à satisfaire pour utiliser l'instruction,
* un message de validation qui est un cryptogramme de la combinaison d'accès.

Le porte clé contient des "autorisations", chaque autorisation étant constituée :
* d'un identificateur d'autorisation,
* d'un paramètre d'autorisation,
* d'une clé d'autorisation qui paramètre l'algorithme cryptographique.

Pour donner l'accès, le porte clé vérifie :
* que l'intersection des identificateurs d'audience reçus et des identificateurs d'autorisation résidents n'est pas vide,
* et que les paramètres de validation reçus sont conformes aux paramètres d'autorisation résidents (date, coûts).

L'utilisation du porte clé peut être conditionnée par la fourniture d'un mot de passe de calcul.
A partir du message de validation et de la clé paramétrée, le porte clé calcule la combinaison d'accès qu'il délivre au terminal.

La spécification comporte, en annexe, le document ISO/TC 97/SC 19/ GT 4 "Proposition du Comité Membre Français - Cartes à microcircuits à contacts - 2ème partie - Protocoles d'échanges" Octobre 1982.

En 1982, l'Administration française proposera au Comité Consultatif International des Radiocommunications (CCIR - Commision d'étude XI) une nouvelle question 37/11 sur les Systèmes de radiodiffusion (Télévision) à accès conditionnel (qui sera prolongée par une proposition de programme d'étude en 1986) (Ref. 4).

Les experts du CCIR sont initialement très hésitants et partagés pour soutenir cette proposition. S'agit-il bien de radiodiffusion ?

La définition de la catégorie juridique du service de Radiodiffusion dans le Règlement des Radiocommunications est la suivante :
"Service dont les émissions sont destinées à être reçues directement par le public en général : "les émissions d'un service de télévision à accès conditionnel sont elles destinées à être reçues directement par le public en général ?"

Les Administrations hésitent.
La conférence des plénipotentiaires de l'UIT (Nairobi 1982) tranchera en décidant que les aspects techniques doivent faire l'objet d'études au CCIR.
Cette question 37/11 est donc inscrite depuis lors à la Commission d'Etudes XI chargée des questions techniques du service de radiodiffusion (télévision).

DEUXIEME PARTIE

LA SPECIFICATION ET LE DEVELOPPEMENT DE LA FONCTION "ACCES CONDITIONNEL" DU SYSTEME MAC PAQUET - 1983 / 1990

La spécification, puis le développement, de la composante "accès conditionnel" du système Mac Paquet auront été particulièrement longs et difficiles.
Ils ont nécessité une persévérance assidue (pour ne pas écrire une obstination têtue !) de la part des experts européens et français, pour atteindre les niveaux technique, technologique et opérationnel (1990) des produits et systèmes actuels.

Ils ont débouché, en France sur le système D2 Mac Eurocrypt, et, au Royaume Uni, sur le système D Mac Eurocypher.

Dans cet exposé, on considérera surtout la situation vue de France, et donc le cheminement qui a conduit au système D2 Mac Eurocrypt.

Néammoins, comme on le montrera, ces deux cheminements eurent une genèse commune, durant la période 83/84 de normalisation du système C Mac Paquet, et sur laquelle on développera quelques rappels historiques.

Vu de France, on peut identifier deux grandes phases dans ce processus :

La première phase va de 1983 à 1987 :
Elle est caractérisée par une ferme opposition des pouvoirs publics français au concept d'une télévision satellitaire à péage selon la norme MAC.
* D'abord, de 1983 à 1985, du fait de leur opposition à la norme Mac elle-même, opposition qui se mue progressivement en soutien, à partir de l'accord THOMSON / PHILIPS de 1984, pour déboucher sur l'accord franco-allemand Mexandeau / Schwarz-Schilling de 1985, relatif à l'usage du D2 Mac Paquet sur les satellites TV Sat - TDF ;
* mais également, de 1985 à 1987, du fait du maintien de l'opposition au concept de télévision satellitaire à péage.

La seconde phase va de 1987 à 1990 :
Elle est caractérisée par un changement progressif de cette ferme opposition en un ferme soutien, avec, en conclusion, la publication en France de l'arrêté Eurocrypt du 28 Février 1990.

A . LA PREMIERE PHASE DE NORMALISATION ET DE DEVELOPPEMENT

Le rôle de l'UER durant la période 1983 / 1984 - Le contexte en France

Le travail normatif conduisant aux parties aujourd'hui communes aux systèmes D Mac Eurocypher et D2 Mac Eurocrypt fut mené, de 1983 à 1985, dans le cadre de la Commission Technique de l'UER, et implanté, en 1984, dans la spécification du système C Mac Paquet.

*Il concerne **l'architecture générale du système, la spécification de l'embrouillage** et du désembrouillage des messages/signaux audiovisuels, **la génération et la synchronisation des séquences pseudoaléatoires** d'em**brouillage à partir des mots de contrôle.***

Il concerne également l'organisation de la gestion des titres d'accès et la distinction des deux fonctions de communication distinctes que sont :
* *le contrôle de la validité des titres en usage (ECM),*
* *l'actualisation des titres existants ou l'introduction de nouveaux titres dans le public (EMM).*

Nous y reviendront plus en détail par la suite.

Mais, en 1984, ce processus normatif se trouva de facto gelé.
Ni en France, ni au Royaume Uni, ni à fortiori en Allemagne Fédérale, les conditions n'étaient remplies pour progresser.

*1 . **Le contexte de la création du Groupe d'Expert V/CA** (début 83) :*

C'est lors de la réunion du Bureau de la Commission Technique de l'UER de Février 1983 que la décision fut prise de constituer un groupe d'experts pour "l'accès conditionnel aux services de diffusion directe par satellite".

On lit, dans le compte rendu de cette réunion (Ref. 5) :
"Il y a en gros deux points de vue au sein du Bureau. Les uns, majoritaires, pensent que tout l'embrouillage et la gestion d'accès (décryption) devraient être communs en Europe ... d'autres pensent que l'embrouillage devrait être commun, mais qu'il sera difficile d'avoir également un système commun de gestion de l'accès, et que, de toutes façons, si tel est le cas, la pénalité de coût sera modeste ...

On expliqua qu'il y avait déjà, au Royaume Uni, un comité qui étudiait l'accès conditionnel, avec l'espoir de prendre une décision en Avril 83. Le Membre anglais fut prié d'expliquer (à ce Comité) qu'une décision prématurée pourrait ruiner la norme commune européenne de DBS, et que c'était l'espoir de l'UER d'obtenir une telle norme commune..."

Il fut convenu que TDF proposerait le Rapporteur de ce Groupe.

Ayant manifesté, en France, un certain prosélytisme en faveur de la création d'un tel groupe, et plus généralement en faveur d'un soutien français à la norme MAC, je suis donc désigné comme premier Rapporteur du Groupe V/Accès Conditionnel. Il faut aller vite, dans un contexte qui, en France, ne peut être mieux caractérisé que par le courrier adressé, le 21 Septembre 1982, au Directeur des Affaires Industrielles et Internationale de la DGT par le Ministre des PTT, Monsieur Louis MEXANDEAU :

"Je vous ai confié une mission de coordination des actions industrielles conduites par la Direction Générale des Télécommunications et par l'Etablissement public de diffusion.

Le Président de la République a annoncé, pendant sa conférence du mois de Juin, le lancement d'un quatrième programme financé par d'autres moyens que la redevance, et le Conseil des Ministres entend, depuis le 7 Juillet 1982, orienter la politique de l'audiovisuel dans trois direction : les satellites de diffusion directe, les réseaux câblés, le quatrième programme. De telles orientations conduisent forcément vers le développement de nouveaux équipements d'usagers qui doivent pouvoir déchiffrer des programmes payants, recevoir plusieurs sons en différentes langues, et décoder des programmes de videographie diffusée.

Les caractéristiques de diffusion devront être choisies de manière que ces nouveaux équipements individuels puissent indifféremment recevoir la quatrième chaine, ou des programmes provenant des satellites de diffusion directe.

Dans ce but, vous voudrez bien former un groupe de travail paritaire composé de spécialistes de l'Etablissement public de diffusion (T.D.F.) et de la Direction Générale des Télécommunications, présidé par un représentant de T.D.F. qui sera chargé d'étudier cette question, et de proposer différentes solutions d'équipements qui, fabriqués en grande série, devraient se situer à un niveau de coût moyen

Bien qu'il apparaisse très difficile - compte tenu des échéanciers prévisionnels de ces programmes (le lancement du satellite pré-opérationnel TDF 1 est alors prévu en 1985) et de l'état de développement des normes et de la technologie - de satisfaire aux exigences définies par le Ministre en s'appuyant sur la norme Mac Paquet en cours de préparation, le Directeur des Etudes et Recherches de T.D.F. conserve, pendant quelques mois, un certain espoir de "compatibilité technique".

Cet espoir repose principalement sur deux constats :
* *les technologies de la videographie diffusée à péage par carte à mémoire ont été longuement étudiés (comme nous l'avons ci-dessus),*
* *il peut exister, au niveau de l'embrouillage du signal video par rotation circulaire, une certaine compatibilité entre le Mac et les signaux Pal/Secam embrouillés : ces aspects seront longuement développés dans une note que Messieurs Marie et Arragon, des Laboratoires PHILIPS du LEP, adressent à l'Auteur, le 9 Juin 1983, sous le titre :*
  "Utilisation du principe de rotation de la ligne active pour l'embrouillage des signaux Mac. Application au transcodage Mac/Secam et Mac/Pal."

Au Royaume Uni, c'est la BBC qui a reçu du Grouvernement la responsabilité de gérer le programme satellitaire. Compte tenu de ce plan d'affaires, la BBC était fermement en faveur de l'utilisation du Pal, avec une sous porteuse numérique (A Pal), mais la commission Part, constituée par le Gouvernement, s'est prononcée pour le système Mac, qui a le soutien de l'IBA et de l'Industrie.

Dans le rapport BBC RD 60 (Ref. 6), de Janvier 1983, rédigé par S.M. Edwardson (et publié sous l'autorité de Ch. Sandbank) sous le titre "Télévision par abonnement, une proposition de système d'ensemble pour le Royaume Uni", on lit :

"La BBC prévoit de commencer l'exploitation d'un service de radiodiffusion par satellite à deux canaux en 1986. Un canal, décrit comme "La fenêtre sur le monde" transportera un signal qui sera normalement transmis. L'autre canal, décrit comme un canal à abonnement, transmettra des signaux qui seront normalement embrouillés, de telle manière qu'ils ne puissent être reçus que par ceux qui auront payé un droit ("charge") additionnel. Un tel droit pourrait prendre la forme d'un abonnement (mensuel) et il pourrait y avoir un système à deux

niveaux, dans lequel un abonnement couvrirait la plupart des programmes, tandis qu'un abonnement additionnel couvrirait, par exemple, un petit nombre de programmes spéciaux, ou "premium programmes", durant le mois.
Le "paiement par programme" n'est pas envisagé, quoiqu'il serait possible avec deux des options qui sont décrites ..."

Le système décrit comporte une carte éléctronique d'abonnement que l'utilisateur insert dans son terminal, et un numéro personnel d'identification (PIN) qu'il reçoit par voie postale et introduit au clavier dans le terminal.

Le document commente les propositions américaines d'adressage par l'antenne, et conclue négativement.

Il examine également les questions de coût du récepteur :
"On estime que la vie de la carte d'abonnement sera longue, probablement plusieurs années. Une carte commerciale, produite par PHILIPS, est adaptée et déjà disponible. Son coût estimé est de 10 £ l'unité, en petite quantité, réduisible à 1 £ l'unité en grande quantité ... Il est difficile d'estimer le coût possible des circuits de désembrouillage tant que les normes DBS n'auront pas été finalement arrêtées ... Cependant, si le traitement numérique du signal video est utilisé dans les récepteurs de télévision domestiques, le coût supplémentaire du désembrouillage peut être relativement faible, si le traitement du désembrouillage est associé à celui du décodage. Par exemple, les traitement de désembrouillage peuvent être relativement communs avec ceux de ré-arrangement et de décompression d'un décodeur Mac numérique. Si des composants CCD sont utilisés pour le décodage des signaux Mac, il est difficile de voir comment les mêmes CCD pourraient être utilisés pour le désembrouillage, et il en résultera des coûts additionnels".

Le Bureau de la Commission Technique, le 10 Février 1983 (Ref. 5), a élaboré une proposition de compromis concernant la norme satellite qu'il fait connaitre sous la forme d'une déclaration (extrait) :

"Le Bureau de la Commission Technique, se basant sur les résultats des études des sous-groupes compétents du Groupe de Travail V, et sous réserve qu'une solution satisfaisante soit apportée aux problèmes mentionnés plus loin aux points (a) à (h), recommande à la Commission Technique d'adopter une norme de diffusion directe par satel-

lite, se fondant sur les éléments suivants :

* système video à codage par composantes avec compression dans le temps,
* système audio à modulation de type C, avec multiplexage par paquets, offrant une capacité d'au plus huit voies audio comprimées de haute qualité,

offrant une possibilité de contrôle d'accès.
Ce compromis, selon le Bureau, ne serait acceptable que s'il en résulte un seul système de diffusion directe par satellite utilisé au sein de l'UER. Les représentants de TDF et de l'ARD/ZDF ont fait savoir que leur acceptagion dépend des progrès qui seront réalisés d'ici à la réunion de la Commission Technique (19 Avril 1983)."

Une réunion exceptionnelle est prévue les 8 & 9 Mars 1983, à Munich (IRT) pour tenter de donner un contenu technique concret à la proposition de compromis élaborée par le Bureau de la Commission Technique de l'UER.

Le tout nouveau Président de TDF fait connaitre aux experts de l'Etablissement Public (MM. Keller, Mathieu, Noirel, Pommier & Guinet) qu'il considère leur participation à cette réunion comme inopportune. Mais, après diverses interventions auprès de la Haute Autorité de la Communication Audiovisuelle, l'interdiction d'y participer sera cependant rapportée.
C'est au cours de cette réunion que les questions techniques principales, qui bloquaient un accord sur une utilisation du multiplexage par paquet (proposé par les experts français) et qui concernait le transport des messages audio-numériques, seront résolues grâce à une proposition de Monsieur Hessenmuller (DBP).

Dans mon rapport de mission (Ref. 7), j'écris notamment :

"Le Groupe V-Ad hoc, chargé de traiter les questions "accès conditionnel aux services satellite", a tenu une réunion préliminaire, en formation réduite (Rapporteurs des sous-groupes de V) (Rapporteur Y. Guinet).

Une lettre à l'attention des Directeurs techniques des Membres a été rédigée. Elle comporte un projet de mandat, une demande de désignation d'experts (pour les Membres qui sont en mesure de contribuer activement), et un questionnaire dont la réponse est demandée pour le 1er Avril 1983.

Ce questionnaire vise principalement à préparer, au plus vite, conformément à la demande du Bureau, l'établissement d'une norme unifiée pour l'embrouillage et le débrouillage des signaux MAC.

Il vise également à collecter l'opinion des Membres sur les fonctions et l'organisation des systèmes d'accès (ex. carte à mémoire) du point de vue de leurs incidences économiques et juridiques.

La prochaine réunion est prévue les 7 & 8 Avril. Je souhaiterais qu'elle puisse avoir lieu en France (démonstration du système Discret).

Une question, qui mérite mérite toute l'attention de TDF, est celle de la compatibilité entre un "péage satellite" et le "péage 4ème chaine SECAM".

Si cette compatibilité pouvait être assurée, au plan fonctionnel comme au plan technologique, il en résulterait **des avantages considérables** au niveau national.

La norme C - Mac - Paquet, et le système DIDON - DISCRET - Carte à mémoire, semblent permettre cette compatibilité. Celà devrait être vérifié au plus tôt au niveau des laboratoires afin qu'il puisse en être tenu compte dans le cadre du dépouillement de l'appel d'offre DIELI en cours."

(Dans une longue note adressée au Directeur Général de TDF (Ref. 8), le 30 Mars 1983, cette position est argumentée et le Directeur des Etudes et Recherches exprime le voeux de pouvoir l'exposer au Groupe qui a été constitué pour dépouiller l'appel d'offres 4ème chaine, et qui est présidé par Monsieur CAYET de TDF).

La réunion de la Commission Technique de l'UER du 18 au 22 Avril 1983 sera particulièrement difficile. Le document UER Com T 488 de mai 83 en retrace le déroulement, et la position que prennent les différents Organismes européens.

2 . **Les travaux du groupe d'expert V/CA en 1983 - 1984**

Nous nous limiterons ici à une brève description des travaux du Groupe d'expert V/CA qui se réunit à Paris (7 & 8 Avril 83), Kingswood Warren (17 & 18 Aout 83) (Ref. 9), Liège (14, 15, 21 & 22 Novembre 83) (Ref. 10) et Bruxelles (17, 18 & 19 Janvier 84) (Ref. 11), recevant, durant cette période, de l'ordre de quatre vingt dix contributions techniques.

Les Experts suivants participent aux travaux (comme Membre ou comme Rapporteur d'un groupe, engagé dans une autre partie de la spécification du système Mac Paquet) :

* *IBA B. Sewter (V1 - EVSS) - T. Long - A. Mason - Lothian - Collins*
* *BBC P. Rainger (V) - Ch. Sandbank (V1 - HDTV) - S. Edwardson - A. Oliphant - R. Ely - N.J. Knee*
* *CCETT L. Guillou - M. Mathieu - Y. Noirel (V2) - Dehery - Lambert*
* *RTVE J.A. Tartajo (V3)*
* *SR A. Nyberg (V4) - K. Engstroem (V4)*
* *RAI Cominetti (V2)*
* *RTBF Bodson*
* *UER D. Wood (Secrétaire) - H. Mertens*

Les résultats de cette activité seront introduits en Février 84, par H. Mertens (Directeur Technique Adjoint de l'UER, et véritable Coordonnateur européen), dans la 5ème édition du document SPB 284 (Ref. 12), spécifiant le système C Mac Paquet "dans le cas de l'usage généralisé des émissions embrouillées, y compris pour l'accès libre", mais également dans un document SPB 316 qui sera adressé à la Commission juridique de l'UER.

Les Figures 1 à 5 en résument le contenu technique.

Un premier progrès est fait à Paris, en Avril 83, avec la rédaction d'un document de synthèse (Ref. 13).

Les progrès les plus importants seront réalisés lors de la réunion de Liège. Dans mon rapport de mission, j'écris, le 30 Novembre 83 (Ref. 14) :

"On a adopté, de façon définitive, la spécification de la forme d'onde du signal Mac embrouillé ... la spécification de principe d'un automate d'embrouillage (et de sa synchronisation) ... et l'on a constitué deux sous groupes d'experts (M. Edwardson (BBC) et M. Long (IBA)) pour finaliser la spécification.

Mais c'est dans le domaine de la structure et de la terminologie pour le contrôle et la gestion des titres d'accès que les progrès ont été les plus importants. La BBC, l'IBA et le CCETT ont proposé, au cours des mois écoulés, des systèmes apparemment différents. L'objectif poursuivi était d'identifier, au delà des apparences, ce qu'ils avaient de structurellement identique, de le dénommer et de le définir.

Cet objectif a été atteint, ce qui a permis :
* de définir une **structure unifiée**,
* de définir le rôle respectif des **clés de distribution** (associées aux porteurs de titres) et des **clés d'autorisation** (associées aux catégories de titres utilisables),
* d'identifier la fonction de deux flux de messages destinés au porteur :
  - les **messages de contrôle des titres (ECM)**,
  - les **messages de gestion des titres (EMM)**,
* de définir, quelle que soit la nature du titre d'accès, les **fonctions à remplir au niveau des porteurs de titres** ."

C'était l'essentiel de ce qui pouvait faire l'objet d'un consencus normatif à ce stade.

En effet, de sérieuses divergences existaient au sein du Groupe pour aller au delà. Sans même parler de la cryptologie elle-même, matière délicate, l'IBA souhaitait utiliser "l'adressage par l'antenne" (Ref. 15) pour la gestion des titres d'accès, ce qui n'était pas, à l'époque, à la portée de la technologie de la carte à mémoire (Ref. 16). Par ailleurs, cette technologie n'était pas suffisamment mature pour obtenir le soutien de nos collègues européens.

Il est utile de rappeler ici que sur proposition du Rapporteur, le Bureau de la Commission Technique de l'UER avait adopté le principe selon lequel toutes les émissions satellitaires, y compris les émissions gratuites, devraient être embrouillées. Les arguments avancés conservent aujourd'hui toute leur actualité (Ref. 17) :
* unicité du comportement technique du système, du point de vue de la qualité de service offerte au téléspectateur, mais également du point de vue de la compatibilité électromagnétique et des rapports de protection.
* unicité des récepteurs (Consumer Electronics) du marché.
* mais, également, meilleure adéquation du système aux exigences spécifiques du média stellitaire (et notamment la possibilité d'occultations nationales) pour satisfaire aux exigences économiques (droits de diffusion), ou autres.

L'adoption de ce principe suscita une vive opposition du Directeur de l'IRT (Centre de Recherche de l'ARD / ZDF), le Docteur U. Messerschmid qui, le 1er Décembre 1983, adresse le telex suivant à Carlo Terzani, Président de la Commission Technique :
"Je recommande fortement l'usage de signaux non embrouillés dans le cas de transmissions à accès libre, pour les raisons suivantes :
1. Les transmissions à accès libre doivent constituer la part principale du DBS (acceptabilité par le public, libre circulation de l'information),

2. Les signaux non embrouillés peuvent être traités, dans le récepteur, aussi bien par des circuits analogiques (CCD) que numériques.
3. Le risque de dégradation de l'image par l'embrouillage (Line-tilt) ne devrait pas être étendu, sans nécessité, des transmissions à accès conditionnel aux transmissions à accès libre.
4. La spécification existante actuelle (C Mac Paquet) peut être maintenue dans ses parties essentielles. Nous n'avons besoin que d'un supplément pour l'accès conditionnel.
5. Les récepteurs capables de ne traiter, seulement, que les signaux non embrouillés sont plus simples et meilleur marché ..."

Au delà des considérants techniques, plus ou moins discutables, on discerne déjà un comportement des radiodiffuseurs publics allemands au regard de ces nouvelles technologies de media qui n'a pas significativement évolué depuis, et dont les fondements juridiques devraient être étudiés.

Un autre résultat du travail du Groupe V/CA aura été la production d'un document de synthèse des aspects techniques et des implications économiques et juridiques de l'introduction de la fonction d'accès conditionnel dans le système de télévision par satellite (Ref. 18). Pour autant que je m'en souvienne, les premières réactions des Juristes seront plutôt réservées. Le fondement de cette réserve est le crainte que les Etats n'utilisent ces techniques pour entraver l'exercice des principes de la libre circulation de la pensée et de la libre réception des ondes. Il est vrai que cette question fondamentale se pose, et que l'utilisation de moyens de cryptologie impose aux Etats, dans ce domaine, comme dans d'autres domaines des télécommunications, la nécessité de mesures nouvelles réglemantant la production et la commercialisation de moyens de cryptologie.
On ne peut pas exclure, dans le contexte politique de l'état de l'Europe de l'époque, que de telles considérations soient de celles qui aient influencé, et continuent d'influencer, la prise de position des radiodiffuseurs allemands.
Rappelons, par exemple, que le 10 Décembre 1982, à la 100ème Assemblée pleinière, l'Assemble Générale des Nations Unies a adopté une Résolution relative aux "principes gouvernant l'usage par les Etats des satellites artificiels de la terre, pour la radiodiffusion directe internationale de télévision". Cette Résolution prévoit que ces activités doivent être menées d'une manière compatible avec les droits souverains des Etats, y compris le principe de non intervention. En Europe, les Pays de l'Est (y compris la RDA) l'ont voté, tandis que la plupart des Pays d'Europe de l'Ouest s'y sont opposés ; la France, l'Autriche, la Finlande, la Grèce, l'Irlande, la Suède et le Portugal se sont abstenus.

B . LE GEL DES TRAVAUX NORMATIFS DURANT LA PERIODE 84 / 87

Cette activité de normalisation de l'UER est, à court terme, en sérieux conflit avec le plan d'affaires satellitaires de l'Etablissement Public de Diffusion.

A l'approche de la réunion de la Commission Technique de l'UER (Vatican Avril 84), le Président de TDF recompose donc sa délégation. Il demande au Directeur du Centre Technique de l'UER de mettre fin aux fonctions du Rapporteur du Groupe V/CA (et du Groupe V1 - Codage numérique de l'image). Dans la lettre de démission que celui-ci lui adresse, le 7 Avril 84, il écrit notamment :

" En tant que Rapporteur du Groupe Ad hoc du Groupe V "Accès conditionnel aux satellites de radiodiffusion", j'ai oeuvré pour que soit prise en compte cette fonctionnalité essentielle du service et pour que soient menés les travaux techniques préliminaires nécessaires dans le contexte européen.

Cette action difficile n'est pas aujourd'hui achevée, mais une meilleure compréhension du problème existe, à la suite des travaux qui ont pu être réalisés au cours de l'année écoulée. Ils devront être poursuivis dans le contexte nouveau créé par l'accord THOMSON PHILIPS.

Nombre de ceux qui étudient les conditions économiques du développement des services de diffusion directe dans le contexte européen considèrent que le financement publicitaire ne permettra pas, durant la première période de croissance du moins, d'assurer leur viabilité économique.

Cette question n'a pas, à ma connaissance, trouvé à ce jour une réponse claire. Je regrette que ces aspects économiques essentiels ne soient pas considérés avec tout le sérieux qu'ils méritent.

Une indication très significative est cependant donnée, par l'intérêt que les professionnels britanniques portent au mode de financement par péage. Et nous avons, en France, Canal Plus.

Je ne doute pas que cette question influencera la suite du débat."

De son coté, la Haute Autorité de la Communication Audiovisuelle, en charge des affaires de l'UER, exprime son ferme soutien à l'élaboration d'une norme européenne unique pour la télévision satellitaire.

L'accord THOMSON PHILIPS du 27 Mars 84 n'a pas encore le contenu technique précis qui prendra ultérieurement la dénomination de D2 Mac Paquet. Les choix techniques et industriels de Canal Plus sont maintenant faits avec Discret 1 pour l'embrouillage (retard variable) et un système d'accès conditionnel simple à secret enterré.

La spécification C Mac Paquet est incompatible avec les choix techniques du plan cable à terminaison optique.
G. Thery vient de déposer son rapport sur le satellite TDF 1.

En Allemagne Fédérale, on préfère évidemment conserver le système Pal, et au Royaume Uni, le programme satellitaire national est en cours de transfert, du secteur public (BBC) au secteur privé (IBA).

Les mois suivants vont être utilisés par le CCETT, avec J. Sabatier, D. Pommier et Alard notamment, pour produire la spécification du D2 Mac Paquet, laquelle reprendra in extenso tous les éléments de la spécification C Mac Paquet relatifs à l'accès conditionnel.

Y. Noirel assure désormais la fonction de Rapporteur du Groupe V/CA de l'UER.

La forte motivation du Ministre de l'Industrie va progressivement conduire à la modification formelle de la position française vis à vis de la norme Mac Paquet, et déboucher sur l'accord Mexandeau Schwarz Schilling de Juin 1985.

Mais, dans la négociation menée, avec l'Allemagne Fédérale notamment, par le Représentant des Pouvoirs Publics français (Monsieur Pomonti), l'accord intervient sur une "spécification réduite" du système D2 Mac Paquet, excluant notamment le format d'image 16/9, et l'accès conditionnel.

En Allemagne Fédérale, le plan d'affaires satellitaires de la DBP prévoyait alors le lancement TV Sat 1 à la fin 86 (il ne sera lancé que fin 87). Les arguments ne manquent pas, compte tenu des délais disponibles, pour "réduire" la spécification, allant ainsi dans le sens d'un D2 Mac Paquet "Super Pal". Les radiodiffuseurs publics sont très opposés à l'accès conditionnel et au nouveau format d'écran. Exposant leur position sur l'évolution des systèmes de télévision actuels, ils écrivent (Ref. 19) : "Il serait absurde de modifier les proportions d'image (de 4 x 3 à 5 x 3 ou 5.33 x 3) simplement "pour montrer au téléspectateur qu'il existe une nouveauté"."

En conséquence de quoi, ITT, seul Industriel des semi-conducteurs en Europe prêt à investir dans cette technologie, conçoit une architecture de composants VLSI, basée sur une première fonction de base (DMA 2270) excluant le désembrouillage et la désanamorphose de l'image, et une seconde fonction complémentaire, voire optionnelle (DMA 2280) pour réaliser ces traitements. ITT n'engage que le développement de la première, celui de la seconde, non spécifique à ce stade, étant renvoyé à une phase ultérieure, non déterminée.

C'est sur la base de cette technologie que le développement de la première génération de produits finis (téléviseurs, syntoniseurs) est engagée par les Industries de Consumer Electronics (PHILIPS - THOMSON - NOKIA). Cette génération se trouvera en porte à faux lors du lancement de TDF 1, par rapport aux décisions du CSA incluant les services à péage de Canal Plus et autres.

Le consensus n'existe pas non plus en Mars 1986, entre les Industriels européens, pour intégrer cette fonction d'accès conditionnel dans le programme EUREKA 95, comme cela figurait pourtant dans la première proposition adressée par le Président de la RTIC, le 11 Mars 1986, à Monsieur Silliard.

EUREKA 95 ne retiendra que la seule composante "haute définition". A cette époque, il manque encore, dans l'Industrie, une juste appréciation de l'importance réelle de cette fonction de communication, et de l'importance des efforts qu'il reste à mener pour la spécifier, et développer ses technologies.

Notons toutefois que LA RADIOTECHNIQUE INDUSTRIELLE & COMMERCIALE avait négocié, en 1986, un contrat d'études avec le CCETT en vue de prédévelopper notamment les fonctions de désembrouillage et de contrôle d'accès par carte à mémoire, sous la forme d'un "récepteur de référence". Cet équipement permettra d'effectuer les premières présentations publiques conjointes de télévision à accès conditionel dans le courant 1988.

C . LA SECONDE PHASE DE NORMALISATION ET DE DEVELOPPEMENT DURANT LA PERIODE 87 / 90 - MAC EUROCRYPT ET MAC EUROCYPHER

Le travail normatif n'est relancé qu'en 1987, par la constitution du Consortium **Euromac** .

On se souvient que des fournisseurs de programme audiovisuel britanniques (CPPG) avaient lancé un appel d'offres pour disposer d'un système de diffusion satellitaire, à accès conditionnel, utilisant la norme MAC et utilisable sur le satellite Astra.
Le consortium Euromac fut constitué par les Industriels pour répondre à cet appel d'offres.

Sans faire partie de son Comité Exécutif, le CCETT et TDF étaient Membres actifs de sa structure technique, et une part significative de son savoir faire résultait des travaux menés dans le cadre du contrat d'étude CCETT - RPIC précité.

Résumons succintement cette seconde phase, qui va porter essentiellement sur la spécification des langages et protocoles télématiques de contrôle et de gestion des titres d'accès.
Nous n'entrerons pas dans l'analyse technique : D'autres sont bien mieux qualifiés, tels, par exemple, Mme Coutrot, Messieurs Blineau, Michon, Marquet, Lenoir, Meillan au CCETT et à TDF, mais également les experts de l'industrie comme Messieurs Höffelt, Ben Dahan, Pellerin, Hellier, Kerjan, pour ne citer que quelques noms au sein du Groupe PHILIPS, ou Monsieur BURGEY au SERICS.
Ce Consortium se présenta publiquement à Montreux, le 12 Juin 1987.
Il établit la spécification technique du second composant ITT (DMA 2275) pour le désembrouillage et la désanamorphose de l'image, et finança la première phase du développement de ce composant VLSI (spécification du 13 Aout 87). Ce Consortium soutenait la spécification D2 Mac Paquet (Ref. 20).

Un second Consortium, dit "anglo nordique", est constitué peu après. Il se dénommera **Cryptomac** .
Le principal lien entre ses Membres, était, initialement, le soutien à la spécification D Mac Paquet, alors en cours de spécification à partir de la norme C Mac Paquet (Ref. 21). Mais il y avait en fait, dans ce consortium anglo nordique plusieurs intérêts d'affaires opposés : BSB, avec le soutien technique de l'IBA, était alors en cours de constitution (un contrat de concession de IBA à BSB de trois canaux pour 15 ans est signé en Juillet 87) et les candidats britanniques écartés se regroupent autour d'Astra.

PHILIPS, qui participait aux deux Consortiums, prit l'initiative (Monsieur van OOSTENBRUGGE) de proposer leur fusion, sous la dénomination commune d'Eurocrypt, et de susciter, par le canal de l'EACEM, la réanimation d'une structure de travail au sein de l'UER. Sa présidence fut confiée au Dr FORREST (IBA).

Par ailleurs, les exigences du plan d'affaires de BSB conduisit cet important acteur britannique, au printemps 1988 (Ref. 22), à quitter la table de normalisation et à retenir, en relation avec General Instruments, un système à secret enterré, dénommé Eurocypher, conforme à son objectif d'affaires : Etablir un réseau national fermé.

Ce choix, accompagné d'une commande importante de composants auprès d'ITT (Ref. 23), eut l'effet de relancer vigoureusement en France l'intérêt pour la technique d'accès conditionnel. Les Pouvoirs Publics demandèrent au Président du CCETT, par ailleurs Directeur Général de TDF (M. MACHUEL) de désigner un expert chargé de finaliser la spécification.
Ce qu'il fera le 8 Novembre 1988, en désignant J. BLINEAU.

Le Consortium Crypto-Mac, que BSB avait quitté, se trouvait également affaibli par le choix du Groupe Murdoch, l'un des principaux locataires d'Astra, en faveur du système Pal Videocrypt.
Enfin, le plan d'affaires d'ITT, mettant les connaissances acquises et les travaux effectués dans le cadre du programme du développement du composant D2 Mac DMA 2275 au service de BSB (DMA 2285) affaiblissait le Consortium Plessey Mullard Nordic VLSI, qui s'était positionné sur le développement de la technologie D Mac Paquet.

Au sein du Groupe Eurocrypt, les tenants des concepts Crypto-Mac se trouvaient donc affaiblis par cette évolution des affaires. Par ailleurs, les différences de conception au niveau de la gestion des moyens de cryptologie, certaines contraintes imposées par l'état de développement industriel de la technologie de cartes à mémoire et microprocessurs, les incidences des choix techniques sur la conception des réseaux télématiques de gestion des titres d'accès, et, plus généralement, l'interaction de ces choix techiques avec les plans d'affaires des acteurs économiques concernés, tous ces facteurs ne permirent pas de fusionner les points de vue.

A l'opposé, durant toute cette période, l'intérêt d'affaires de Canal Plus et celui de France Telecom s'étaient progressivement éveillés. Ils avaient d'abord passé contrat entre eux, et avec TDF, pour que le CCETT apporte à Canal Plus une expertise technique dans les études relatives à l'usage du D2 Mac Paquet en émission de Terre.

Le 9 Juin 88 (Ref. 24), le Président Rousselet adresse d'ailleurs une lettre circulaire exprimant l'intention de Canal Plus d'abandonner le système à module de sécurité immatriculé, retenu en 84, en faveur d'un système à module détachable.

L'ETAC, organe technique des Industriels européens de Consumer Electronics déclare, les 6 & 7 Octobre 88 (Ref. 25) :

* ETAC confirme à nouveau sa préférence déjà exprimée en faveur d'un standard européen unique, qui devrait être EUROCRYPT ;
* ETAC regrette qu'un radiodiffuseur européen (BSB) ait l'intention d'adopter un système non européen ;
* ETAC a été informé de ce que le radiodiffuseur français Canal Plus a adopté la spécification Eurocrypt Mars 88 ;
* le Consortium Eurocrypt validera maintenant la spécification Eurocrypt Septembre 88, et étudiera la compatibilité mutuelle de ces deux versions.

Le 11 Janvier 1990, J. Blineau a été en mesure de recueillir le soutien des principaux acteurs économiques français au choix de principe de la solution Eurocrypt - Mars 88, laquelle servira de base à l'arrêté du 28 Février 1990 (Ref. 26), aux décisions du CSA d'Avril 89 et aux plans d'affaires subséquents de Canal Plus et de France Telecom.

Joseph Blineau précise, dans son rapport final :

"Le système Eurocrypt retenu permet plusieurs modes de commercialisation des services ou des programmes de télévision payante. Il a été organisé pour aussi permettre de regrouper sur un seul module de sécurité plusieurs opérateurs de service, sans que leurs méthodes de commercialisation soient liés. Enfin, il possède des capacités à évoluer.

Les méthodes de commercialisation disponibles pour chaque opérateur sont

* l'abonnement à la durée :
  cet abonnement multi-programmes peut être organisé en niveaux ou en thèmes. Les dates de départ et de fin sont fixables usager par usager.
* le paiement à la séance :
  le paiement peut se faire à l'avance, ou de manière impulsive. Chaque séance est identifiée par un numéro.
* le paiement à la durée :
  qui, comme l'achat de séance impulsif, demande un compteur sécurisé dans le processeur du terminal ("boite à jetons").

La distribution des autorisations (titres d'accès) peut se faire par l'antenne (par le signal D2 Mac Paquet lui-même), sans que cela soit obligatoire.

Le partage du module de sécurité permet à chaque opérateur de disposer de ses propres clés dans chaque carte d'abonné, pour le contrôle ou la gestion des titres d'accès. Ce partage n'est pas obligatoire si un opérateur veut disposer de sa propre carte. La contrepartie est alors, pour l'usager, d'avoir à changer de carte en changeant de canal. Pour les opérateurs partageant une famille de cartes, il est nécessaire d'ordonner un minimum de la vie de la carte, mais ce minimum ne contient pas la commercialisation des programmes. Il ne contient que la gestion de base de secrets à long terme et permet l'introduction de nouveaux opérateurs au cours de la vie de la carte. Ceci suppose l'existence d'un organisme (autorité émettrice) qui définit l'usage des cartes partagées."

CONCLUSIONS

1 . La décennie 1980 - 1090 a été marquée, en Europe, par des transformations profondes du cadre juridique de l'économie de media audiovisuel.

L'économie de droit public, qui prévalait initialement, a fait progressivement une place croissante, dans la plupart des grands Pays européens, à une économie de droit privé.

Simultanément, la révolution technologique, comme résultat de trente années de progrès scientifiques inimterrompus, imposait la conception d'une nouvelle génération de médias audiovisuels.

En oeuvrant pour orienter l'évolution du système de radiodiffusion de l'avenir, l'UER manifestait donc un sens élevé de l'intérêt collectif, car il était aisé de pressentir que le résultat de ces oeuvres ne serait pas mis au profit exclusif des radiodiffuseurs de droit public.

Certes, les objectifs formulés étaient en avance de plusieurs années sur l'état de la technologie européenne, mais ils étaient clairement définis et, comme le montre la situation actuelle, accessibles à elle. Le développement de la technologie fut ainsi encadré pour atteindre les objectifs qui avaient été formulés.

C'est le milieu, et l'organisation des affaires, qui en déterminera les formes.

2 . Dans le media audiovisuel, la fonction télématique de l'accès conditionnel n'est pas une fonction annexe. C'est une fonction de base dont le rôle essentiel apparaîtra plus clairement à l'avenir.
Elle rendra économiquement possible les perfectionnements ultérieurs du média.
Mais surtout, en permettant des formes diversifiées de rétroaction de l'usager sur le serveur, elle permet d'espérer à l'avenir un meilleur exercice des libertés de communication audiovisuelle.

3 . L'histoire de la normalisation d'un système européen ouvert de télévision à accès conditionnel montre la complexité du processus par lequel le milieu interagit avec la production de la technologie de media.

BIBLIOGRAPHIE ET REFERENCES DIVERSES

Nota : la liste des nombreux (90) documents de travail technique du Groupe UER V/CA figure en annexe au document B.Tech 204 - 211 & 232. Certains d'entre eux seulement sont cités ci-apès.

1 . **Radiodiffusion-Télévision - n° 40 - Nov.Dec. 75**
Numéro spécial sur les "Nouveaux services de Communication sociale"

2 . **Etude TDF 5312 A - Mars 1980**
Structure de contrôle d'accès aux services de teletexte.
J. Gregeois - G. Bernède

3 . **LAR/CAS/100/82/LG - 6 Octobre 1982**
Addendum à la spécification Didon Antiope pour le contrôle d'accès.
Louis Guillou

4 . **CCIR - Commision d'Etude XI - Service de Radiodiffusion (télévision)**
Question 37/11 - Programme d'études 37 A/11.

5 . **Commission Technique 458 - Février 83**
Réunion du Bureau de la Commission Technique de l'UER.
Déclaration sur les normes satellites (10.02.83)

6 . **BBC - RD 60 - Janvier 83**
Subscription Television : a proposed outline system for the UK
S.M. Edwardson

7 . **Rapport de mission - Y. Guinet - 10.03.83 - DE/DIR/53/41/83/YG**
Objet : mission des 8 & 9 Mars 1983 à l'IRT (Munich)

8 . **Note au Directeur Général - Y. Guinet - 30.03.83 - DE/DIR/53/83/YG**
Objet : Péage - Normes satellites - Appel d'offres "Terminaux lère chaine"

9 . **B.Tech. 204 - Aout 83**
Rapport sur la seconde réunion ad hoc V/CA - Kingswood Warren 17 & 18 Aout 83

BIBLIOGRAPHIE ET REFERENCES DIVERSES

10 . **B.Tech. 211 - Décembre 83**
Rapport de la troisième réunion du Groupe ad hoc V/CA
Liège 14, 21 & 22 Novembre 1983

11 . **B/Tech. 232 - Février 1984**
Rapport de la quatrième réunion du Groupe ad hoc V/CA
Bruxelles 17-19 Janvier 84

12 . **Commission Technique 490 - 5th revised version - Draft n° 4 - Feb. 84**
Television standards for 625 Lignes 12 Ghz satellite broadcasting
Version A : generalised use of scrambling, even for free access transmissions.

13 . **Commission Technique 486 - Avril 83**
Contribution du Groupe ad hoc du Groupe V : Systèmes de radiodiffusion à accès conditionnel - Considérations générales.

14 . **Rapport de mission - Y. Guinet - 30.11.83**
Objet : Mission à Liège du 14 au 22 Novembre 1983.

15 . **Groupe de Travail V/CA 036 - IBA**
Proposal for a DBS over-air adressed conditionnal access system having a minimal validation cycle time
A.G. Mason

16 . **LAR/CAS/225/83/LG - Louis Guillou - 8 Novembre 83** - GT V/CA 059
Note de synthèse sur l'accès conditionnel en radiodiffusion.

17 . **V/CA 065 - 8 Novembre 1983 - Y. Guinet**
L'accès conditionnel constitue-t-il une fonctionnalité de base ou une fonctionnalité annexe ddu service de radiodiffusion directe par satellite en Europe ?

18 . **SPB 316 - Fev. 84 - RDS à accès conditionnel** - Principes généraux quelques considérations techniques, éconmiques et juridiques (Contribution du Bureau de la Commission Technique).

19 . **Clarification et explication de la position adoptée par les radiodiffuseurs publics allemands ARD et ZDF** dans le débat sur la future norme de production TVHD.
Revue Technique de l'UER - Février 87

BIBLIOGRAPHIE ET REFERENCES DIVERSES

20 . **Juin 87 - Euro Mac Consortium**
Présentation aux fournisseurs de programmes, aux opérateurs de satellites, et aux PTT nationaux
Montreux - 12 Juin 1987.

21 . **2 Juin 87 - Communiqué de presse de l'IBA**
La télévision par satellite et le système Mac.

22 . **10 Mai 88 - Communiqué de Presse de BSB**
BSB annonce ses plans relatifs à l'industrialisation des récepteurs DBS.

23 . **11 Mai 88 - Communiqué de Presse de Intermetall**
BSB commande des composants de décodage D Mac à ITT

24 . **9 Juin 88 - Lettre circulaire du Président de Canal Plus**
Module de sécurité pour télévision payante.

25 . *ETAC 1988/40 - EACEM / ETAC*
Statement on conditionnal access for TV Broadcasting.

26 . **Arrêté Eurocrypt** - 28 Février 1990.

LISTE DES FIGURES

Extraits du document B.Tech. 232 (Rapport V/CA - Liège - Nov. 83)

Figure 1

Access control subsystem

(Note 3)

CLK2
D
VAL

Packet Demultiplexer (with buffer store)

Decryption sub-system

Local validation signals

x bits

Control word

Free-access receiver

Local control word system

F/N
VAL

Load
PRBS1
CP

F/N
Line freq.

Load
PRBS2
CP

Basic PRBS generator

D
CLK2
VAL

y bits

8 bits

To vision decoder and descrambler

Load
PRBS3
CP

CLK2*
(Note 1)

Sound/data descrambler

1

To other decoders

Useful data

Packet demultiplexer (with buffer store)

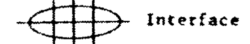
BC/BI detection

(2)

Descrambled signal to sound decoder

BI

Ex-or (mod. 2 adder)


Interface

Note 1 - CLK2* is the same clock used to extract the useful data from the buffer store.

Note 2 - In App. 3 to GT V/CA 042 (Fig. 1) a separate descrambling unit is foreseen for data messages (e.g. subtitling, teletext).

Note 3 - Includes processing of entitlement checking and management messages.

Fig. 1: NOTIONAL BLOCK DIAGRAM INCORPORATING THE BASIC FUNCTIONS OF THE "ACCESS CONTROL" DBS SOUND/DATA

(Note: this system does not represent a system proposal, but is for discussion purposes.)

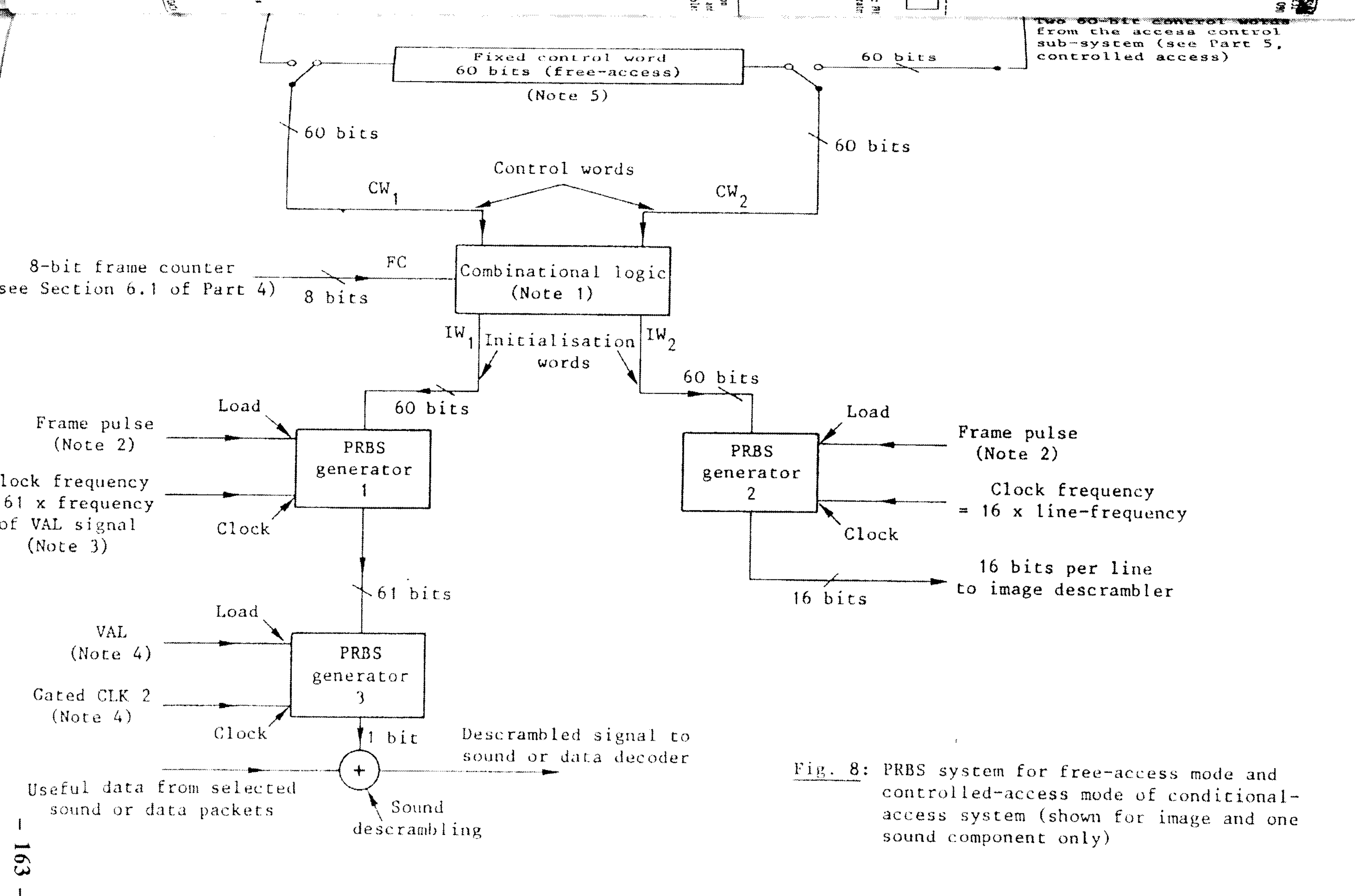


Fig. 8: PRBS system for free-access mode and controlled-access mode of conditional-access system (shown for image and one sound component only)

Figure 3

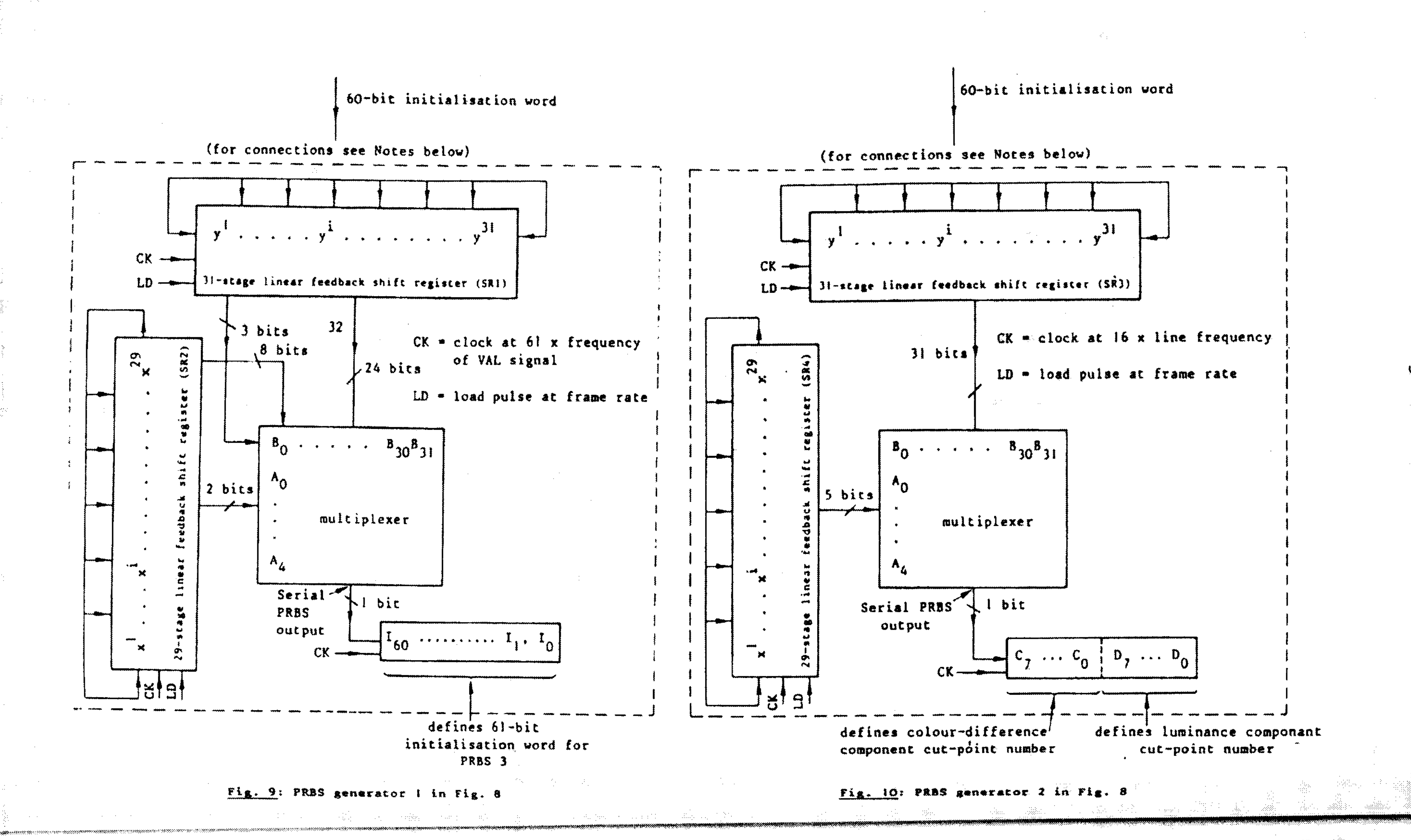


Fig. 9: PRBS generator 1 in Fig. 8

Fig. 10: PRBS generator 2 in Fig. 8

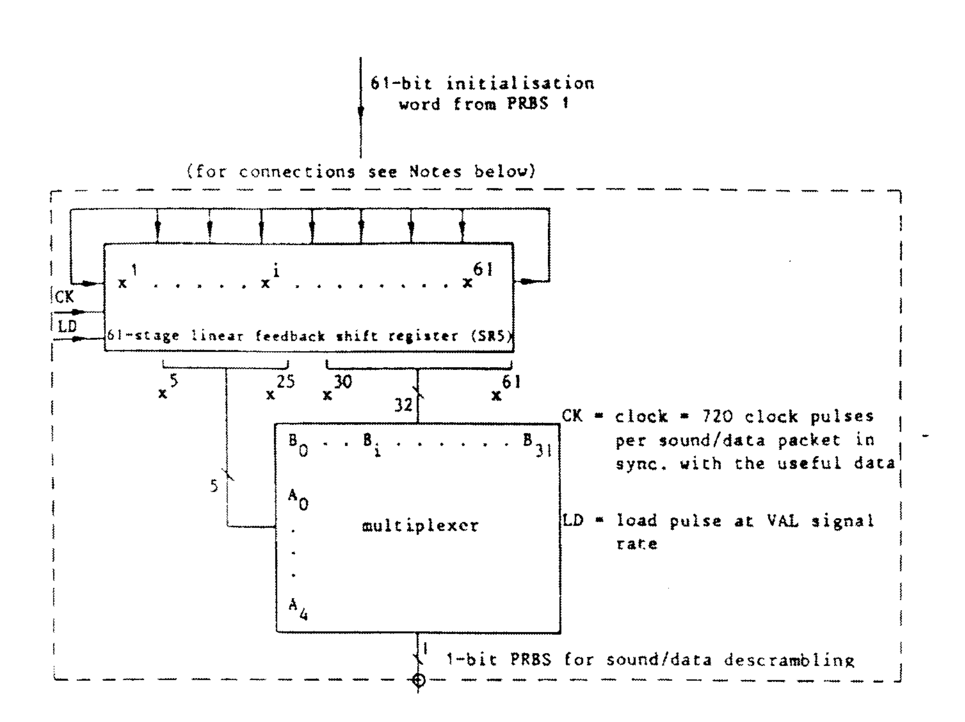
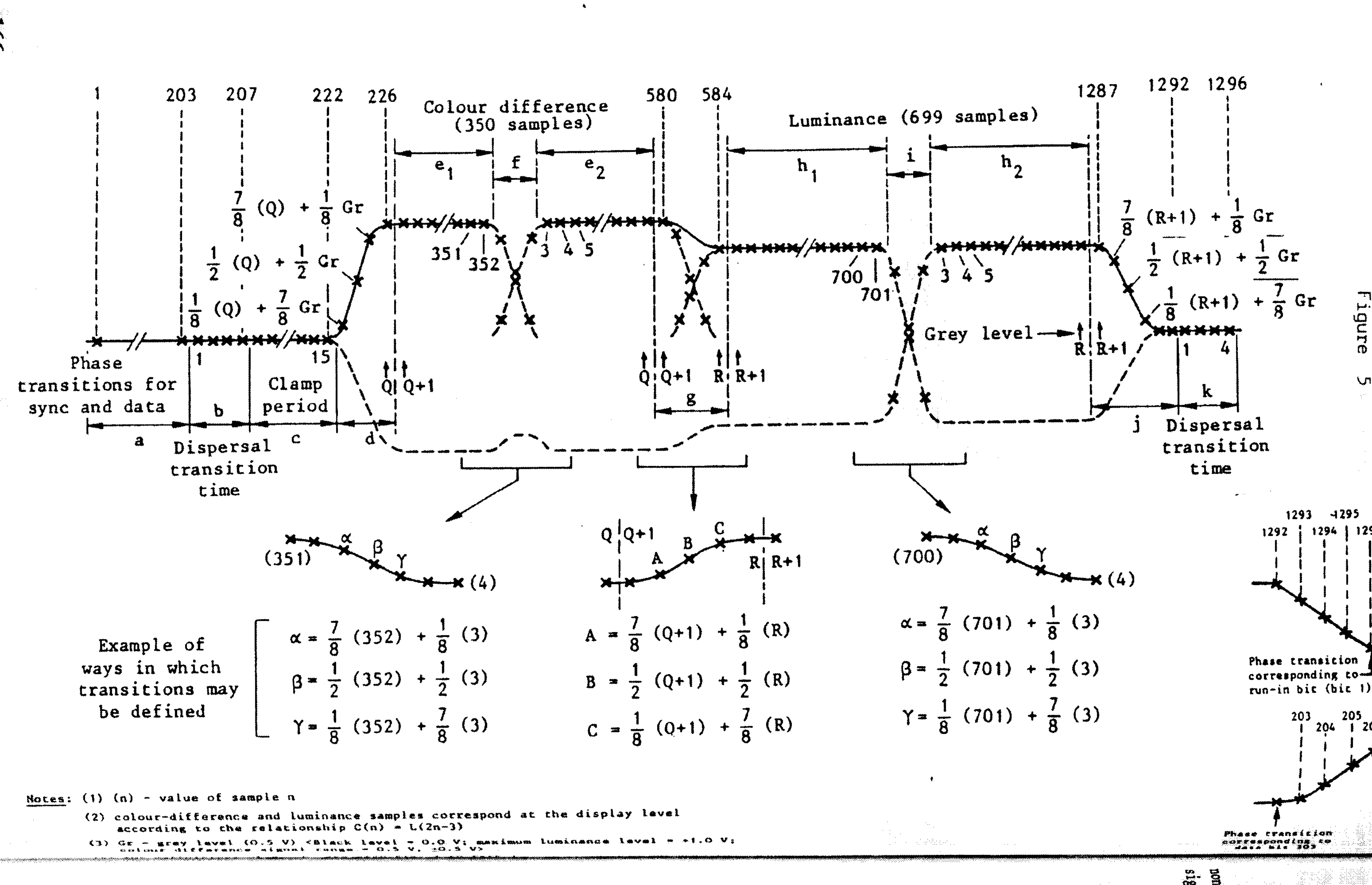


Fig. 11: PRBS generator 3 in Fig. 8

Figure 5



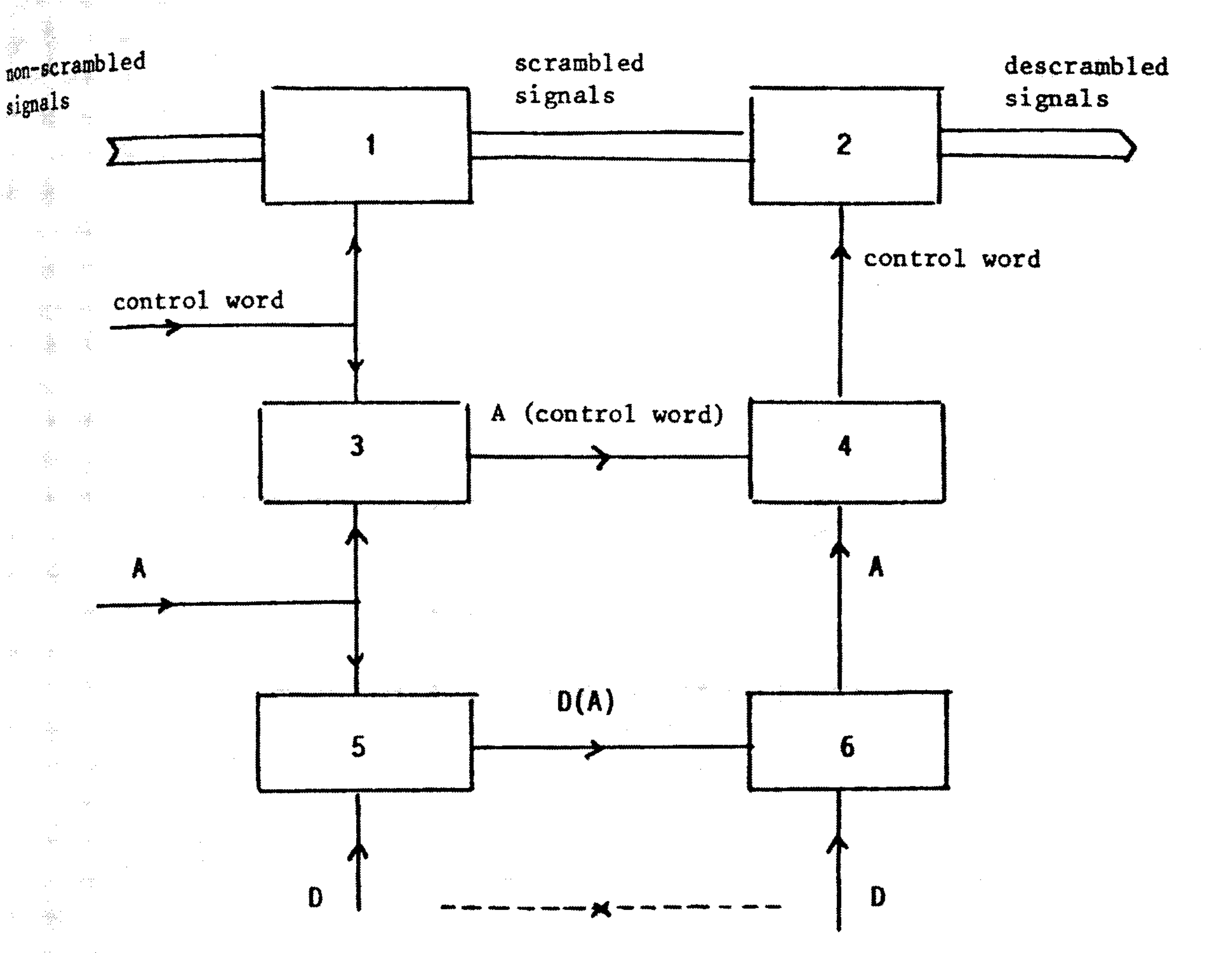
Notes: (1) (n) - value of sample n

(2) colour-difference and luminance samples correspond at the display level according to the relationship C(n) = L(2n-3)

(3) Gr = grey level (0.5 V) (Black level = 0.0 V; maximum luminance level = +1.0 V; colour difference signal range = -0.5 V, +0.5 V)

Figure 6

GENERAL PRINCIPLE



1,2 scrambler and descrambler

3,5 encryption unit

4,6 decryption unit

A authorisation key associated with a service

D distribution key associated with an entitlement support

A(control word) control word encrypted by an authorisation key

D(A) authorisation key encrypted by a distribution key

OPERATION OF EUROCYPHER SYSTEMS

CURRENT EXPERIENCE

AND FUTURE DEVELOPMENTS

Philip **BAGENAL**, Steve **UPTON**
British Satellite Broadcasting Ltd
Marcopolo Building
Queenstown road
LONDON SW8 4NQ
ROYAUME UNI
Tél : +44 71 978 2222

Chris **BENNETT**
VideoCypher Division
of General Instrument Inc
6262 Lusk Boulevard
SAN DIEGO, CA 92121
ETAS UNIS
Tél : +1 619 455 1500

TABLE OF CONTENTS

OPERATION OF EUROCYPHER SYSTEMS: CURRENT EXPERIENCE AND FUTURE DEVELOPMENTS

Philip Bagenal, Steve Upton - British Satellite Broadcasting Ltd
Chris Bennett - VideoCipher Division of General Instrument Inc

1 Introduction

British Satellite Broadcasting Ltd (BSB) provide conditional access for their signals using the Eurocypher system developed by the VideoCipher Division of General Instrument Inc. The system architecture and features provided by Eurocypher are discussed in [Bennett90]. In this paper, we discuss the operation of the system in more detail.

The paper is divided into two parts. In the first part, the implementation of BSB's system is discussed. Both BSB's Customer Management System (CMS) and their Subscriber Authorisation System (SAS) and Programme Control Systems (PCS) are reviewed. In the second part of the paper, a number of other possible Eurocypher system management architectures are discussed, to illustrate the issues involved in providing service for multiple programmers, for programmers providing service to several countries, and for programmers supporting IPPV services. This section closes with a brief review of issues involved in coordinating Eurocypher conditional access with other access control systems.

2 The BSB Installation

2.1 Customer Management System

With a ready market of 21 million homes owning televisions in the UK, the potential for Direct Broadcasting by Satellite offering subscription television is enormous. BSB's business plan projects a penetration of several million customers within a few years. When the infrastructure required to support BSB's operations was considered, it was immediately apparent that a powerful Customer Management System (CMS) was required and that the system could not be built as an in-house development, in the time available.

The CMS that now exists is a combination of systems from two suppliers, selected through a tendering process. They are CableData, who provide more than 50% of the cable administrative systems in the US, and Next, who run one of the foremost mail order operations in the UK, and who also provide "Own Credit Card" administration to many retail organisations throughout Britain. A joint company, British Satellite Systems (BSS), was set up by CableData and Next to manage BSB's customer operations.

The CMS provides BSB with the financial management of their customers, and with the ability to exercise the various Eurocypher functions available through the interface to the SAS. It is based on large non-stop transaction processing systems with very high reliability and integrity. These are backed up by a telephone response facility capable of handling high volumes with peaky traffic distributions. These aspects of CMS operation are described in the remainder of this section.

2.1.1 System Configuration

The account management for customers is handled by Cabledata equipment; the system (called Quickdata 1000) is based on 32 bit NCR chips and offers the unique ability for every user on the system to secure 1 megabyte of central processor memory. This system provides very fast response times and also enables batch processing to be run in parallel with on-line access. Because each megabyte is a separate CPU board (easily replaced) the effective architecture is of a non-stop nature with 20 minutes worth of battery backup for switchover contingency in case of power failure. This twenty minutes also enables tidy closedown of files if alternative power supplies are not available.

The system can be grown in step with the volume of customers, so processors and disk storage are added as requirements demand. Data is distributed across disk drives in such a way that contention for disk access is minimised.

BSS has now installed 133 x 1 Mbyte processors and 32 x 380 Mbyte disk drives to cater for the first six months of customer growth. In addition there will be a secondary machine after the first 3 months of live running which will act as back up.

The database holds an account for each customer and acts as a sales ledger for billing purposes. In addition it holds a considerable amount of demographic data and also holds details of equipment owned or rented by the customer with services established against each receiver. A very flexible and sophisticated report generator allows reporting on the data, both for ad hoc purposes and for regular Management Information and Financial reporting.

2.1.2 Customer Financial Management Strategies

BSB has defined a range of policies for the financial management of their customers. These policies were forged in co-operation with BSS, to take advantage of the joint experience of the BSS partners in managing customers. They also took account of considerable research into customer management in Europe (including Canal Plus in France), America (Cable and Satellite operations) and mail order, credit card accounting and TV rental in the UK.

Customers who subscribe to BSB's movie service are billed monthly, a month in advance. No customer can receive more than two months of viewing before being cut off from the subscription channel. In order to familiarise UK consumers with the concept of pay TV, a free month's viewing of the movie channel is being offered for the first year or so of the franchise.

Customers are encouraged to pay by direct debit because it is easier and cheaper to administer, and leads to less bad debt. Customers can also pay by credit card, at banks or post offices, or by sending cheques directly to the customer management centre where payments are processed to bank transfer level by automated cheque encoding equipment. Rental customers can also pay at rental outlets where they rent BSB equipment. In order to support this last facility, an automated payment interface has been developed which allows rental organisations in the UK to transfer monies directly to BSB systems.

A considerable marketing operation is backing the launch of BSB, funded by the highest advertising and promotional expenditure for a new product in this century. Since all BSB customers must register with BSB before they can acquire service, even if they do

not wish to subscribe to the Movie Channel, a complete subscriber database is available to support marketing efforts. Initially, simple lists of responders to advertising were generated, but customised marketing systems have now been developed to allow more sophisticated processing of this data. Because marketing systems and associated data require very flexible design features, a prototyping procedure has been developed. Marketing systems are prototyped on BSB computers (DEC VAX's) before they are transferred to mainframes at BSS, which occurs when volumes demand larger storage and processing capacity.

2.1.3 Customer Support

In this section, we describe the functionality provided by the system from the customer's viewpoint.

Initially a customer might telephone to enquire about BSB services. His address will be validated against a national address register, for security and for accuracy. This address register is generated from the electoral register for the UK and is kept up to date annually by Wescot Data Services. It can also be used for credit checking, although with the low level of individual debt that is involved in subscription TV this is not done on a universal basis.

After address capture, the customer will be mailshotted or directed to his nearest retailer, if he has not already purchased or rented equipment. Once the customer has acquired equipment he will have it installed and will contact the customer management centre to have his equipment enabled. Until the equipment is enabled, the customer will only be able to see a message indicating that he should call the customer management centre for service, and giving the phone number. This message is broadcast by the PCS on each channel to all those receivers which are not authorised for any BSB service.

From the moment the customer is first enabled, he will follow a cycle which will both bill him, and maintain the authorisation of his individual equipment through the Eurocypher system. The cycle is repeated for as long as he owns the equipment and continues watching BSB's programmes. The initial enablement identifies the equipment to the Subscriber Authorisation System (SAS), which then transmits a message which is identified by the address of the ACM in the customer's receiver where it is decoded. The message identifies the services which the customer is entitled to view, and enables the receiver to descramble these services. Subsequently the customer can upgrade to further services, or downgrade to remove services. Either action will result in a further system message changing his access rights. At any time he can be sent a screen message based on his service rights or lack of rights; these messages can encourage him to ring the Customer Management Centre for further services or can indicate programming status. It is also possible to send a customer individual messages addressed to his receiver; however this facility has to be used with discretion, because it has considerable volume implications.

Customers can exercise parental control in their homes by requiring input of a personal identification number (PIN) or password for programmes which exceed a user-selectable rating threshold. Each customer can select his own PIN; however, should he forget his PIN he can ring the customer management centre and a system message can be sent to his receiver via the SAS resetting their current PIN to a default value. This allows the customer to input a new one.

If a customer moves house and takes his equipment with him, a change of address will be input on the CableData system, and a message will also be sent to his receiver indicating the new location. This enables programmes to be blacked out in certain areas should BSB choose to use this facility in the future.

If subscription customers fail to pay for more than two months the CableData system will automatically generate system messages for the SAS downgrading those customers from pay services until their accounts have been cleared.

Finally, if a customer sells his equipment or disconnects for any other reason (eg repair), a message can likewise be generated for the SAS disabling the equipment for all services ready for the next user of the equipment.

2.1.4 Telephone Support System

The realtime nature of customer interaction and the planned growth to a large subscriber base in a few years requires the support of a large telephone system manned by many operators. Sophisticated modelling, and some educated estimation, was used to determine what level of manning and telephone positions to implement. This modelling broke down the level of estimated response for each call type into mail response and telephone calls, and also imposed a number of parameters governing call behaviour: the seasonal characteristics of equipment purchase; the capacity available for installing BSB equipment; the customers' response behaviour; and finally advertising patterns. The analysis determined the duration of each type of call and the distributions of calls received by month of the year, day of the week and finally hour of the day, taking into consideration the random nature of the frequency of incoming calls.

From this data, the model estimates the number of positions required to man the busiest hour of the year to provide a response level of 99.9% of telephone calls answered in 2 seconds. This figure gives the actual hardware requirements and the worst case personnel requirement. The distribution of calls determines the personnel requirements at other times. This model allows BSS to optimise their staffing levels and thereby to run their operation as efficiently as possible.

The maximum capacity figures eventually predicted by the model are reflected in the following table. These are currently being tested against actual BSS operations.

Year	Telephone Calls (millions)	Items of mail (millions)	Telephone positions
1	1.75	1.75	150
2	6.00	2.50	250
3	8.00	4.00	270

2.2 The Conditional Access System at BSB

This section describes the particular configuration of Eurocypher equipment which has been implemented by BSB and highlights how the architecture chosen meets the requirements for a reliable, high capacity, high availability system. All elements of the conditional access equipment have been provided by GI, including all components of the Eurocypher uplink systems and the embedded Access Control Modules for the receiving equipment.

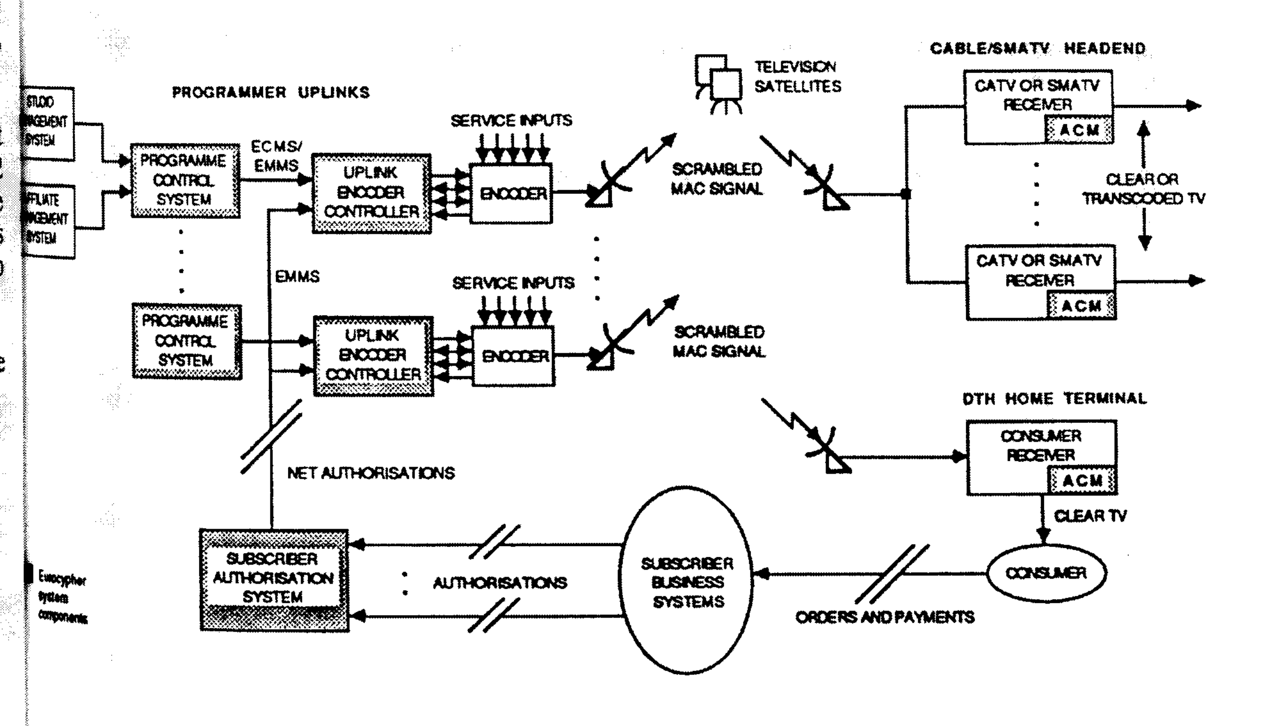


Figure 2.1

EUROCYPHER SUBSCRIPTION SYSTEM ARCHITECTURE

Figure 2.1 shows the three basic elements of the Eurocypher uplink systems which have been implemented by BSB. The uplink equipment consists of an SAS system whose main function is the granting of authorisation rights to DTH receivers as requested by the Business Systems. PCS systems control the conditional access aspects of both TV programme output and data services and finally Uplink Encoder Controllers provide the interface between the conditional access computers and the Tandberg Telecom D-MAC encoders.

As with the initial selection of the conditional access system itself and its supplier, the philosophy which underlies the choice of the system implementation has been one of providing a first class conditional access service which is both reliable and secure.

2.2.1 The SAS

2.2.1.1 Hardware Architecture.

For the SAS BSB have chosen a VAX cluster architecture with two processor nodes. The processors are VAX 6210s which have been selected to achieve both the required transaction rates for processing authorisation requests from the Business Systems and also a satisfactory category rekey rate. The cluster architecture is shown in figure 2.2.

Mass storage for the cluster is a 2.4 Gbyte disk array consisting of four physical drives. For data security these drives are configured as two volume shadowed pairs, one pair for the system files and the second for data. This configuration therefore provides up to 600 Mbytes of storage for the DTH receiver database which is sufficient to support several million users.

The cluster is completed by the addition of duplicated Hierarchical Storage Controllers (HSC) and appropriate peripherals.

2.2.1.2 System Facilities

The SAS provides the capability for the management of large numbers of ACMs within a single Eurocypher category. Units in this category are normally DTH units. It is also possible to operate non-DTH units within the SAS category if required, however. For the BSB application, all receivers, DTH, Cable Head End, SMATV and DataVision are managed by the SAS. It was felt that this approach has a number of operational advantages both in terms of offering a uniform professional customer service facility to all customer groups and the greater versatility arising from operating receivers in a common, shared, category.

The currently installed system supports 55 tiers in the DTH category which are available for programmers' use. This will be upgraded in the near future to the full 512 tiers available within the category.

In addition to the SAS functions listed below as being supported across the Business System interface, the current system provides a number of other features. These include the ability to send Personal Messages, which are Eurocypher text messages addressed to individual receivers, and the broadcast of Nationality Control messages. Personal Messages are relatively expensive in terms of available system bandwidth if used in any

quantity. This facility needs, therefore, to be exercised with discretion and so is not generally used operationally. This feature also provides an extremely useful function for test purposes.

Nationality Control messages broadcast the table of ratings to be used for the parental control facility. This type of message is received by an ACM when it first accesses the Eurocypher message stream and thereby establishes the ratings to be used by the receiver. Since this facility is controlled by an over the air messaging process, it may be varied from time to time and also from country to country as circumstances dictate.

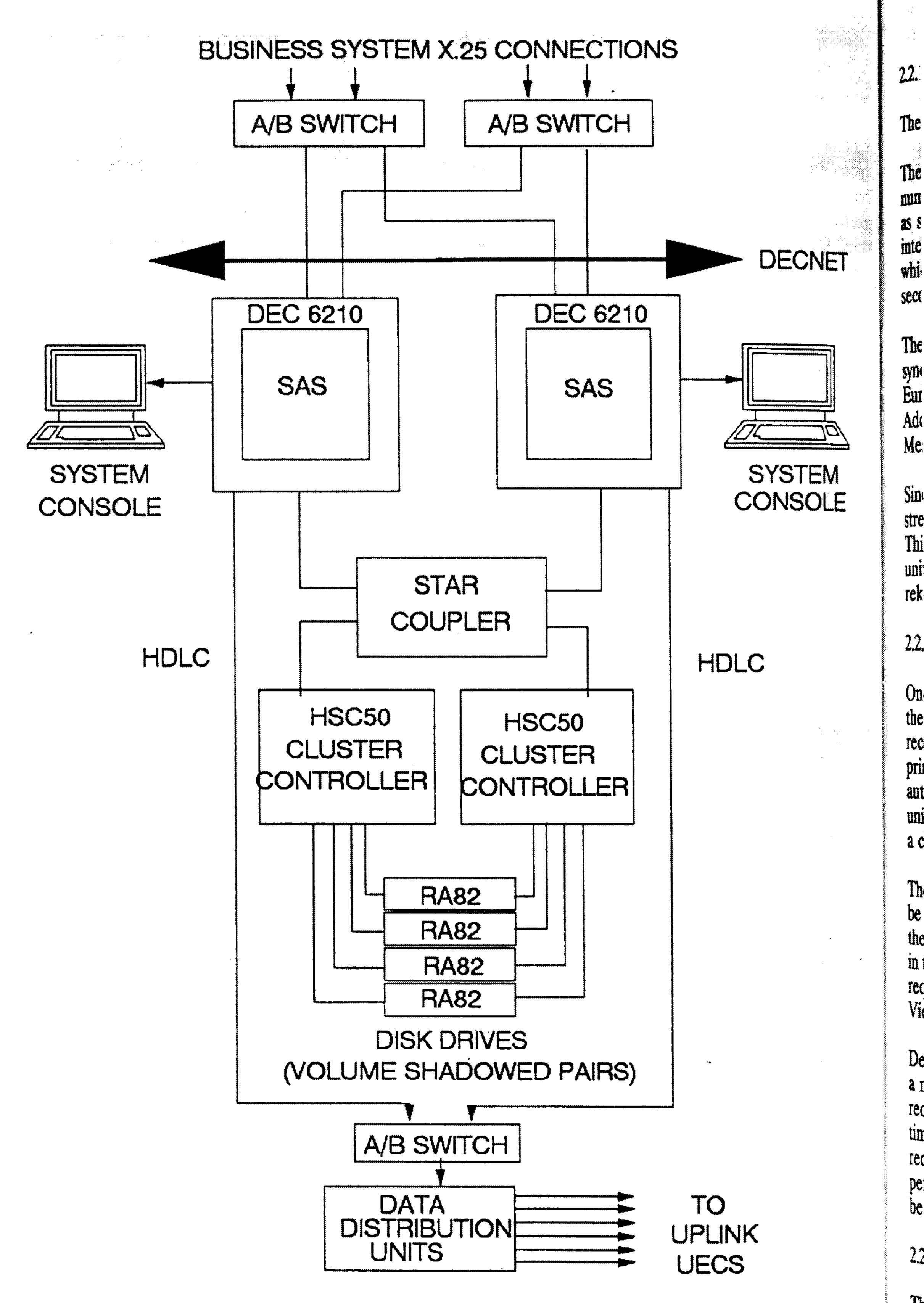


FIGURE 2.2 BSB SAS CONFIGURATION

2.2.1.3 Interfaces.

There are two principal external computer interface types to the SAS.

The first of these provides the links to external Business Systems and will accept a number of the Eurocypher Business System transactions. Those currently supported are as shown in figure 2.3. In the BSB implementation, there are two instances of this interface. One is used to respond to all the television service authorisation requests which are dealt with by the BSB customer management centre described earlier, and the second is used for BSB DataVision customers.

The second interface is from the SAS to the UEC and is currently a 64 kbit per second synchronous link operated using HDLC formats. This link carries the various Eurocypher message types which are generated by the SAS to the UEC such as Unit Addressed Category Rekey messages, Personal Messages, and Nationality Control Messages.

Since the SAS is broadcasting authorisations for the DTH category, a single SAS output stream is distributed to all the UECs in the Uplink via a Data Distribution Unit (DDU). This unit provides one to seven mapping of the data and in the BSB application two units are cascaded to provide the required ten outputs. This architecture ensures that rekey updates are received no matter which BSB channel is being watched.

2.2.1.4 System Transaction Performance.

One of the main system performance parameters of interest is the transaction rate on the Business System interface, as this governs the rate at which changes in the state of receivers can be made. Usually, this implies a change in the authorisation state, but in principle it can mean any change, for example in the unit's location. Changes in the authorisation state of an ACM will normally arise from two sources, either because the unit is a new one and is being granted its initial set of access rights or because there is a change in the services which have been purchased.

There will always be a background rate of both of these transaction types which must be catered for in the rate capability of the interface between the Business System and the SAS. These rates must also take account of daily, weekly and seasonal variations in the rate of customer activity. However, the main determinants of the underlying rate requirements are the growth of the receiver population and the use of Advance Pay Per View (APPV) events.

Detailed modelling of all these factors has led to the establishment of a requirement for a minimum transaction rate of 1 per second. This will meet BSB's projected business requirements for at least three years. Measurements on the total combined processing time of both the CableData business system and the SAS indicate that this minimum requirement has already been exceeded for a typical transaction mix. Current system performance of both the CableData Business System and the SAS is therefore likely to be adequate to meet the foreseen business requirements for a number of years.

2.2.1.5 Rekey Rates.

The SAS rekey rate is defined as the interval between routine category rekey messages

addressed to an individual receiver. It does not include high priority rekeys (known as "instant trips") or changes to a unit's authorisations. For correct operation of the Eurocypher system, it is necessary for an ACM to receive at least one valid category rekey message per rekey interval, normally one month. In practice, because of extraneous factors such as, for example, potential transmission errors or receivers being turned off, it is a system design aim to address each receiver a number of times each month. Typically, this minimum value should be five or six times.

Based on a linear extrapolation from the current system performance, a potential subscriber base of 10 million users would be addressed approximately once every few days.

TRANSACTION	FUNCTION
Sign On/Off	Provides a Log On/Off facility to the Business System
Define New Unit	Sets the initial authorisations for a new ACM
Change Unit Authorisation	Changes the authorisation state for an existing ACM
Change Unit Location	Sets a new location for an existing ACM
Reset Password	Resets the receiver password back to original value
Monitor Unit	Reports the current ACM status back to the Business System
Instant Trip Unit	Sends an instant authorisation to an ACM

FIGURE 2.3 EUROCYPHER FUNCTIONS SUPPORTED BY THE BUSINESS SYSTEM INTERFACE.

The system is currently tuned to handle large numbers of new units and relatively low levels of rekey traffic, since this mix is appropriate to the rapid population growth phase in which BSB is currently operating. Once the population is more stable, as would be more likely with 10 million subscribers, the relative priorities of the different message types can be adjusted to match the prevailing conditions. In addition, there is a planned upgrade to the SAS output data path to double the data rate. The combination of these factors will yield a proportionate increase in the rekey rate.

Both of these potential improvements, plus the excellent performance currently being delivered by the system, means that rekey rates are never likely to be a limiting factor in the growth of the consumer base.

2.2.1.6 Redundancy

Unlike the PCS or UEC, a failure of the SAS, or any of its peripheral systems, does not have an immediate or direct effect on the BSB broadcast operation. The redundancy strategy which has been adopted is therefore different from that used for the other components of the conditional access uplink system.

Failure of the SAS results in the loss of routine rekey traffic and the inability of any Business System to authorise new units or change the authorisation state of existing units. With the rekey rates currently being achieved the former would only become a problem after a very extended period of down time. The latter demands a recovery in minutes rather than seconds or hours, in order to continue to provide satisfactory service to customers.

The redundancy strategy is therefore based on the duplication of all hardware, data, and communication circuits operating in 'warm standby' mode. Thus, two VAX processors are used in the cluster with the Working machine running the application and the Standby machine powered and running but without the application software loaded. Data is stored on a Volume Shadowed disk set. One pair of disks holds all the system files while the second pair contains the data files. Thus, in the event of failure of a single physical drive, there is no loss of data or processing capability. Incoming and outgoing data circuits may be manually switched between one machine and the other and these circuits are themselves provided with a redundant back up.

With this configuration, a mean time to repair (MTTR) of around 10 minutes is easily achievable. In order to continue to provide service to customers during this period, the Business System has a buffer which is used to store transactions which cannot be sent to the SAS. In this way the failure becomes entirely transparent to the viewer, and on re-establishment of the service, the buffer is emptied and processed in the normal way.

2.2.2 The PCS

2.2.3 Hardware Architecture

Figure 2.4 shows the PCS configuration for a single channel. Each PCS application runs on a dedicated DEC MicroVAX II machine. These are standard rack mounted units with the addition of a number of proprietary cards. Each MicroVAX is equipped with both a tape drive and a 140 Mbyte disk drive.

A single PCS is capable of operating one of BSB's five channels. In practice, for resilience to failures, two PCS's are used on each channel working as main and standby.

Data is entered into the PCS application either through one of the four dedicated terminals, or via one of several computer interfaces.

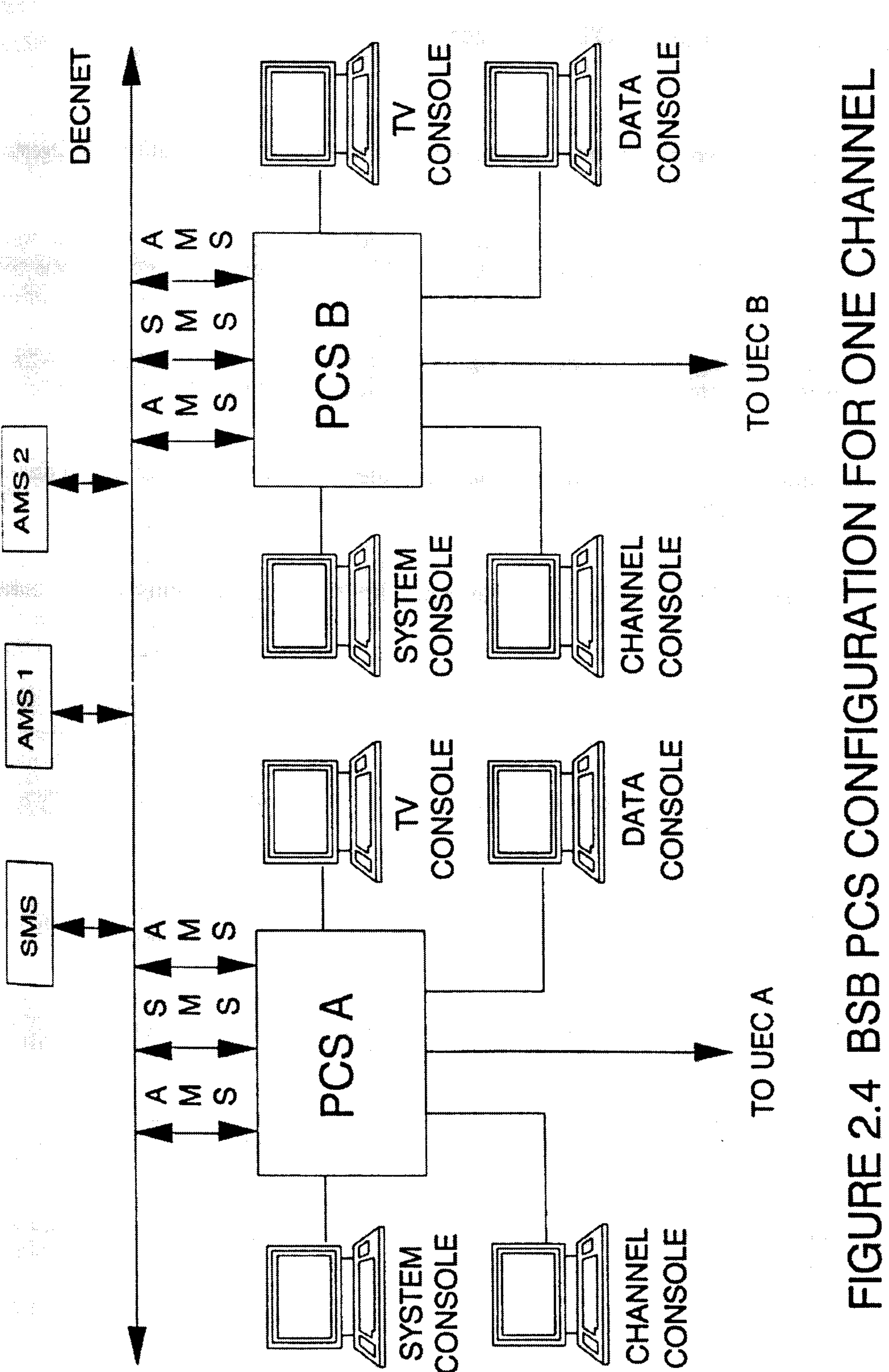


FIGURE 2.4 BSB PCS CONFIGURATION FOR ONE CHANNEL

2.2.3.1 System Facilities

The PCS provides two major functions: generation of Eurocypher programme control information, including that for data services, and authorisation for non-DTH category ACMs.
For the BSB application, the authorisation facilities are not generally used since all BSB receivers are operated in the DTH category.

2.2.3.2 Interfaces

The PCS supports two types of external control interface: the Studio Management System interface, and the Affiliate Management System interface.

The Studio Management System interface provides the primary means by which programme information is supplied to the PCS. It connects the PCS to the BSB automated playout control systems via a DECNET link. The playout systems download programme schedule information including the name of the programme, its duration, parental control rating and the access rights required to view the programme. This information is correlated with the playout of the video and audio material to ensure a consistent, coordinated result on the viewers receiving equipment.

The programme control information is loaded some time in advance of actual playout. Typically, three programmes are loaded ahead of current time. This margin provides adequate resilience in the event of failure of the playout control systems since the system can continue to run without further intervention for the duration of these three programmes. However, there remains the capability to undertake edits to the schedule without the need to alter large numbers of programmes. This makes the system able to respond to any last minute schedule changes required by the programmers in a rapid and flexible way.

The PCS also provides the facility for up to two Affiliate Management System interfaces. These allow the connection of other computer systems which provide the facilities of a Business System for the authorisation of receivers in the channel specific, non-DTH category. These are not used at BSB.

2.2.3.3 Redundancy

Since a PCS failure could have an immediate effect on the broadcast system, the redundancy strategy adopted for the PCS machines is slightly different from that described for the SAS. The two PCS's on each channel are operated in a full hot standby redundancy configuration. Both are constantly operational and providing Eurocypher data streams to their respective UECs. Both have identical programme schedules loaded from the Studio Management System and run with the schedules nominally synchronised. Since loading of the programme information is essentially a non real-time operation there is no difficulty in keeping both machine's databases in step with each other. Additionally, both machines on a channel are operated in 'Key Synchronous' mode whereby both are generating identical programme key data. This allows a change over from one PCS to its standby to occur during the course of a programme without loss of crypto-sync in the receiver.

Generally, one PCS is coupled to one particular UEC. This means that a PCS change

over also results in a UEC change over and therefore, by virtue of the one to one connection to the encoder, these change over as well. However, an additional system feature is that one PCS can be configured to operate with either UEC on the channel. When activated, this mechanism allows the failure of a PCS to leave the remainder of the broadcast chain unaffected.

The final protection against failure is that on the loss of an incoming data stream from a PCS, the UEC will autonomously revert to fixed key operation in order to maintain an encrypted broadcast transmission.

2.2.4 The UEC

2.2.4.1 Hardware

The UEC is designed to provide the interface between the Eurocypher computer systems and the Tandberg Telecom MAC encoder. It is a 19 inch rack mounted unit with its own chassis and power supply. Each UEC contains a seven card assembly based on a standard VME bus.

2.2.4.2 System Functions

The primary functions of the UEC are:

- Interfacing to the PCS and SAS computer systems
- Golay encoding and MAC packetising input EMM and ECM messages
- Mixing and distributing the input control channel streams
- Generating Control Words and providing them to the Encoder

2.2.4.3 Interfaces

Figure 2.5 shows the UEC interfaces which are currently supported for a single channel. These are synchronous links to a PCS and, via a Data Distribution Unit, to the SAS, and the Control Word and ECM/EMM links to the D-MAC encoder.

The UEC architecture and construction allows a straightforward upgrade path to permit the addition of extra interfaces as required by new demands on the system performance. This would include, for example, supporting a second SAS stream or the generation of more than the current 32 control words.

2.2.4.4 Redundancy

As with the PCS, the UECs are duplicated on each channel and are operated in hot standby mode. Generally a UEC failure will be automatically detected by the encoder to which it is connected. The encoder may be configured to respond either manually or automatically and switch over to the standby encoder and hence the standby UEC.

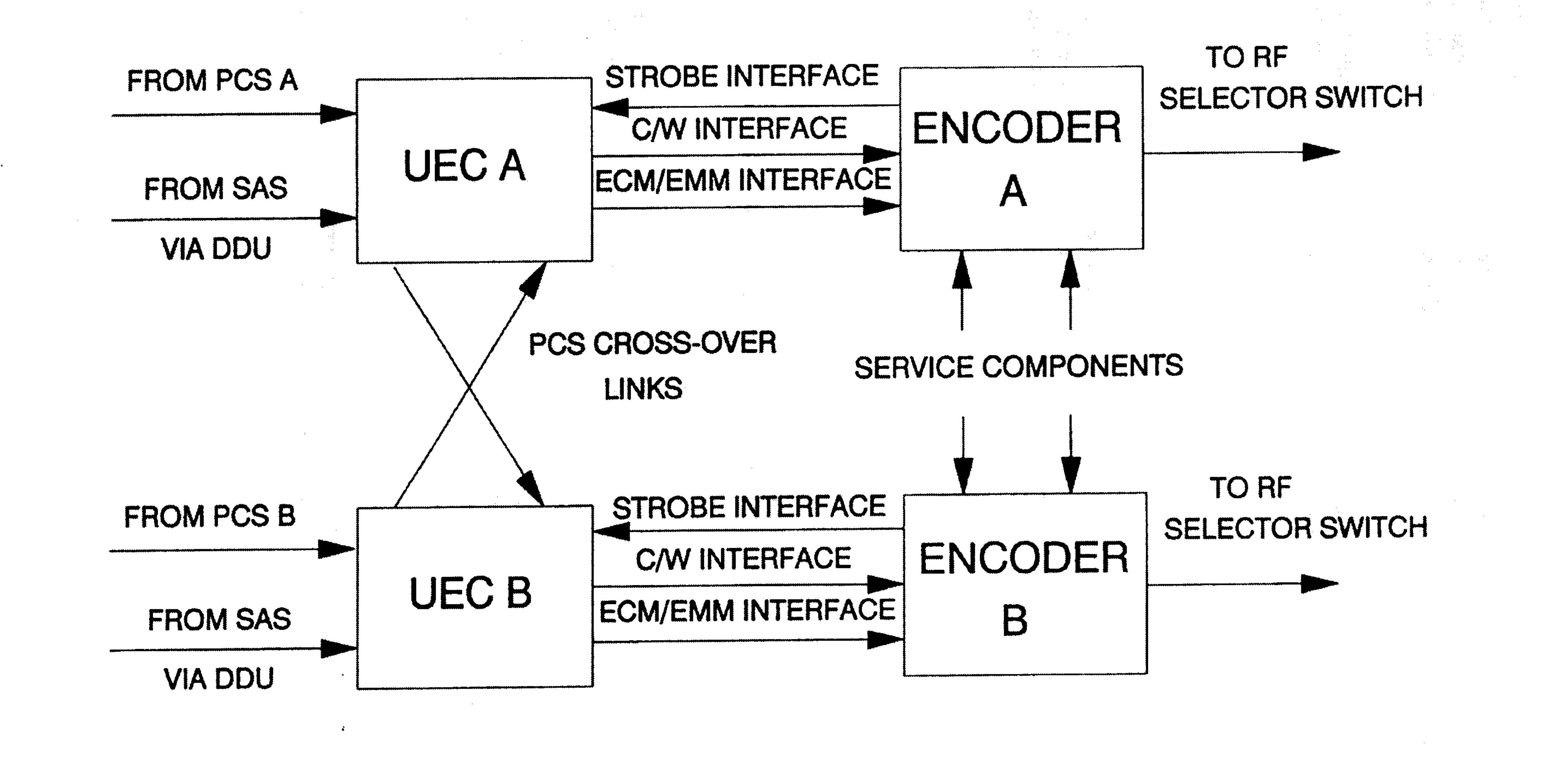


FIGURE 2.5

BSB UEC CONFIGURATION FOR ONE CHANNEL

3 Extended Eurocypher System Management

3.1 Multiple Programmer Support

The Customer Management System described above supports the business activities of a single Eurocypher programmer, albeit one which supplies a large number of services. The Eurocypher system allows the activities of business systems supporting many different programmers to be coordinated through a single SAS. The mechanisms used to achieve this are described in this section.

The Eurocypher SAS, which accepts and processes the authorisations provided by BSB's CMS, is based on the VideoCipher DBS Center software, which currently provides similar services for 17 business systems representing 70 different American and Canadian programmers. The consumer's right to access several of these programmers is not bought directly, but through packaging arrangements which result in the possibility of a consumer being authorised for a programmer several times through different business systems. In North America, 56 programmers are currently supported by more than one business system. Thus, the business systems may support one or more individual programmer, or one or more programmers consortia. A business system may act as a clearinghouse, co-ordinating the authorisations of a number of other business systems.

The VideoCipher DBS Center ensures that the authorisations from different business systems are properly coordinated, so that a descrambler only sees the net authorisation: a service is available if authorised through any business system, and ceases to be available to the user only when deauthorised by all business systems. The Eurocypher SAS supports the same capability. With the adoption of Eurocypher by other MAC programmers, orders for authorisation of their services can be accepted by the SAS from their business systems. The net authorisations are generated by the SAS, and then distributed to the ACMs. Confidentiality of a programmer's subscriber data is assured through separation of the business systems from each other and from the SAS. Neutrality is assured through operation of the SAS by a separate organisation. In North America, the DBS Center is operated by a subsidiary of the VideoCipher Division; the current SAS is operated by European Satellite Services Ltd (ESSL), a consortium of General Instrument, BSB and, other participating programmers.

As described in [Bennett90], the Eurocypher ACM is a member of a single category at a time, and thus has access to 512 tiers. The SAS, as currently implemented, supports a single Eurocypher category, which provides tiers for all services available to ordinary consumers in the area supported by the SAS. Each separately authorised programmer is allocated tiers from this category. The allocation of tiers is determined by the partners of ESSL. From time to time, tiers may be deallocated because they are no longer needed for their original purpose. When this occurs, all ACMs possessing the tier are deauthorised for it, and the tier is not reallocated until this deauthorisation is completed securely.

The SAS also provides facilities for managing the activities of business systems. A business system is only permitted to authorise ACMs for the tiers assigned to the programmers represented by that business system. As the set of programmers represented by a business system changes, so the set of accessible tiers changes. With suitable upgrades to the SAS, a business system can be denied access to ACMs which are bespoke to organisations not represented by the business system. From time to

time, business systems may be removed from the SAS if they cease to be active.

The authorisation messages generated by the SAS are distributed to the uplinks of all channels associated with the DTH category authorised through the SAS. There they are multiplexed into a single MAC packet stream with any authorisation messages generated by the PCS or other SASes and broadcast on the channel. In this way, an ACM can acquire its authorisations regardless of the channel it is listening to. This characteristic allows an ACM in standby mode to update its authorisation and keys on any Eurocypher channel.

3.2 Distributed SAS Architecture

In North America, a single DBS Center is sufficient to support the business activities of all programmers in the continent. Canadian authorisations are collected through a single system which acts as a national clearinghouse, which appears to be an additional business system to the DBS Center in San Diego. This same model could be applied elsewhere. However, while a single DBS Center is sufficient to support all VideoCipher authorisations in North America, it has always been apparent that the more complex political structure of Europe was unlikely to admit the same arrangement.

The Eurocypher system design allows the SAS function to be split amongst several authorisation centres, while still assuring that each ACM can receive all its authorisation updates in a single message from a single SAS. In this section, the architecture of a decentralised Eurocypher authorisation system to achieve this is outlined.

In a distributed system, each SAS would handle authorisations for the programming services of a single country or related group of countries (e.g. France, Scandinavia). Each SAS would operate independently of the others, providing authorisations for consumers residing in that country. All programmers active in the area served by the SAS would naturally establish marketing organisations serving the same or subsidiary areas, and would establish business systems for the same area. The local marketing organisation of a programmer with multinational interests would supply the authorisation data for the programmer's local customers to the local SAS, just as would the marketing organisation of a programmer serving only the area supported by that SAS.

The same approach could be used to support the authorisation activities of rival independent Eurocypher consortia addressing consumers in the same target national market. As an example, consider the case, shown in figure 3.1, where a single country may be supported by more than one SAS. For example, each SAS might support ACMs for rival consortia based on use of different receiver technology. If the receivers of the first consortium could process the signals of the second, the first consortium might grant the SAS of the second consortium the right to authorise its ACMs for the services of the first consortium. A business system supporting the first consortium could then accept subscription orders from any consumer. Authorisations would be directed to the appropriate SAS, based on the type of receiver used by the consumer.

As currently implemented, all ACMs supported by an SAS are placed in the same category. In a network of distributed SASes, each SAS could manage a separate category, or all SASes (or a subset) could be within a common category. A separate category for each SAS allows each SAS to provide access to a complete set of 512 tiers

However, a multinational programmer would then require a separate tier in each region for which service was provided; since these are in separate categories, a separate ECM would be needed for each category on the service, which could slow acquisition time. If agreement is reached to allow the SASes to operate within a common category, then each SAS must be configured to allow authorisations only for tiers allocated to programmers who operate in the region served by the SAS.

Since each ACM belongs to a single category, the value of the system to the consumer is maximised if a large number of services of interest to the consumer use tiers from the pool available to a single category. The advantages of providing rapid consumer access to a wide variety of services in a single DTH category have been demonstrated by the growth of the market for C-band consumer television in North America. Programmers in the United States and Canada have found that the advantages of a single free consumer market in which all programmers can compete on equal terms outweigh the advantages of tied markets which are segmented by commercial and technological means.

The principles of message distribution from distributed SASes are shown in figure 3.1. The authorisation stream generated by each SAS would be distributed to all the uplinks for the programmers associated with the SAS, by any appropriate means, for example as a MAC data service. At each uplink, the authorisation stream is combined with the authorisation streams of any other SASes associated with the same programmer, inserted into the MAC waveform by the UEC and broadcast to the consumers. From the consumer viewpoint, the same result is seen as is seen with a single SAS: the customer receives the authorisations intended for his ACM no matter which Eurocypher channel is being watched.

As a result of this process of multiplexing, the consumer can be assured that all Eurocypher MAC channels carrying services for his area will carry authorisations. However, additional steps are needed to ensure that an ACM which is looking for an authorisation stream can find one carrying authorisations from the SAS maintaining that ACM. Each authorisation message carries an identifier for the SAS which originated it; this denotes the "home SAS" of the ACM which receives the message. At a low rate, each SAS also sends a broadcast message which includes the same identifier. By searching for this identifier, an ACM can assure itself that it has found a channel that should also be carrying its authorisation updates.

A process is also defined which allows an ACM to move smoothly from the jurisdiction of one SAS to that of another. Each ACM is normally "held" to its home SAS; when held, the ACM will ignore authorisation messages from any other SAS. When the user of an ACM moves from an area served by one SAS to that served by another, the home SAS must first "release" the ACM before the new SAS can take hold of it. The SAS will not release an ACM till all business systems authorising the ACM indicate that it is safe to do so. This allows for proper deauthorisation or transfer of subscriber records to take place before service is resumed in the new area.

The configuration of the SAS also takes into account the position of the SAS within the distributed system. Each SAS can be restricted so that authorisations will only be accepted for ACMs coming from a given set of regions, within the 64 regions available in Eurocypher. Along with the identity of the SAS, each SAS will also broadcast programme rating tables and currency representation data for all regions within its franchise area. The set of ACM addresses supportable by an SAS is restricted to the set of addresses available in the SAS keylist; thus, movement of ACMs can be confined to this area by ensuring that other SASes do not possess the same ACM addresses in their keylists.

COUNTRY A

PROGRAMMER UPLINK

CONSUMERS

BUSINESS SYSTEM

BUSINESS SYSTEM

SUBSCRIBER AUTH. SYSTEM

ENCODER

ENCODER

ENCODER

CONSUMERS

BUSINESS SYSTEM

BUSINESS SYSTEM

SUBSCRIBER AUTH. SYSTEM

COUNTRY B

CONSUMERS

BUSINESS SYSTEM

BUSINESS SYSTEM

SUBSCRIBER AUTH. SYSTEM

DISTRIBUTION OF AUTHORISATION TRAFFIC

COUNTRY C

PROGRAMMER UPLINK

CONSUMERS

BUSINESS SYSTEM

BUSINESS SYSTEM

SUBSCRIBER AUTH. SYSTEM

ENCODER

ENCODER

ENCODER

Figure 3.1

PRINCIPLES OF DISTRIBUTED SAS COMMUNICATIONS

3.3 Management of Impulse Pay Per View

The Eurocypher system installed to date supports subscription services and can be used to support a call-ahead pay-per-view service. With the addition of a suitable reportback mechanism and an IPPV Management System (IMS), the system can support Impulse Pay Per View (IPPV). The features made available by the IPPV enhancements are described in [Bennett90]. This section describes the management infrastructure required to support an IPPV system.

The reportback mechanism may be a telephone sidecar, a smart card reader, or other means. At this time, following US experience, it is expected that IPPV reportback will be based on telephone delivery, but different mechanisms may well be appropriate for different countries. It is currently assumed that the IMS and initial telephone reportback units, when fielded, will be based on the equipment currently in operation to support IPPV in the United States. The following description is based on the current American system.

The IMS resides on a VAX computer in a similar configuration to the SAS. The architecture is centred on the IMS, which acts both to coordinate the credit and view history limits of the ACMs and as a central regional data collection centre, in which purchase data is verified and authenticated and then distributed to the business systems supporting IPPV.

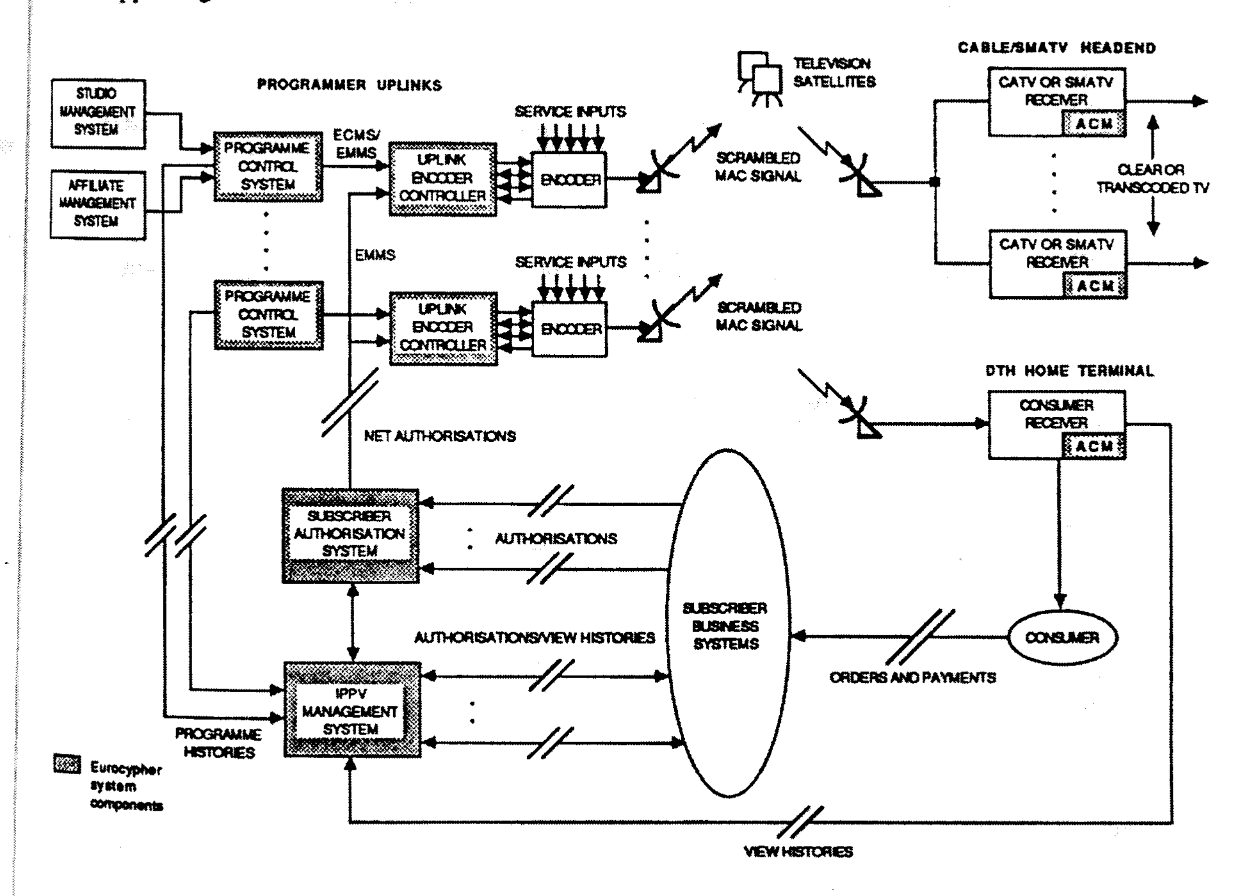


Figure 3.2

SYSTEM ARCHITECTURE OF EUROCYPHER IPPV SYSTEM

The flow of data in the system is outlined in figure 3.2. In order to initiate IPPV service, the consumer must establish an account with one or more business systems supporting IPPV. These business systems then authorise the ACM through the IMS, which establishes limits for credit and unreported view history in the ACM. As programmes are purchased, programme identifiers are logged in the ACM's view history stack and are reported to the IMS. The IMS also receives logs of the playout of purchasable programmes - "programme histories" - through the PCS. As view history data is reported, the ACM's stack and credit limit is advanced by the IMS. The view history and programme history data is uploaded to the business systems authorised to receive it.

Data is reported from an ACM to the IMS through a telephone sidecar. The sidecar accepts data dumps from the ACM, sorts out what has not been successfully reported to the IMS since the last transmission, and relays this information back to the IMS via a phone line for proper accounting. The business system, through the IMS, can poll the sidecar at any time to obtain current view history data. The sidecar can also be configured over-air to report specified data automatically to a specified phone number. The sidecar is told what amount of unreported data is sufficient to trigger a report, when it should attempt to make a report, and how often it should retry if the first attempt fails. The sidecar maintains an internal clock to synchronise these activities. When this algorithm is activated, the sidecar will spontaneously call the designated phone number without being explicitly polled through a control channel.

As with the SAS, the IMS function can be distributed over several computers covering a number of regions, if required.

3.4 Interworking with non-Eurocypher Conditional Access Systems

Since Europe has not standardised on a single conditional access system for satellite television, it has been necessary to consider the issues raised by the existence of several operational systems within the same market. In this section, these issues are discussed, and various options for overcoming the danger of fragmentation arising from competing systems are considered.

For PAL signals there are now several actual and potential systems providing conditional access. For MAC systems, three conditional access systems are recognised by the EBU in addition to Eurocypher. At the moment, the only choice available to the consumer wishing to watch two services differentiated by choice of technology is to buy additional equipment. With appropriate packaging, a multi-system receiver could be built which reduces the complexity and cost somewhat. However, the present state of development appears to carry a real risk of market fragmentation along technological lines. Since the set of services available to a subscriber through any single set of equipment is limited by the choice of technology, the overall attraction is reduced, and the growth of the European satellite television industry may well fail to meet its true potential.

Partly in order to provide a path to address these issues, certain upgrades have been proposed to the Service Identification (SI) portion of the MAC specifications. The packet address and service associations of EMM streams and ECM streams have been augmented by descriptors which identify the type of conditional access system supported by the EMM and ECM streams. In addition, facilities have been defined

which allow for ECM streams supporting different conditional access systems to be associated with the same set of service components.

Using these identifiers, a receiver accessing any MAC signal can select the EMM and ECM streams appropriate to the conditional access system or systems supported by the receiver. This allows a multi-standard receiver to select the access control module required to provide access to the service selected by the user. The receiver could be carrying on activity related to more than one system at a time: for example, if a channel carried a Eurocypher EMM stream, in addition to services scrambled under a different system, background authorisations for a Eurocypher ACM could be obtained while processing access requirements for one of the services with another module.

The same facilities allow a programmer to operate a multi-standard service. This is made possible by the fact that all MAC-compatible conditional access systems conform to a common interface for providing control words. Therefore, with suitable uplink equipment for generating control words and distributing them through all appropriate conditional access systems, the programmer can in principle make a single service accessible to several different types of system.

This route is most likely to be of interest to programmers whose signal is received in countries with different conditional access systems. Using these techniques, the signal can be decoded correctly in each country using the conditional access system authorised in that country. For example, a sporting channel carrying sound tracks in several languages could choose to make each sound track available under a different conditional access system, while the video - common to all sound tracks - would be made available under all systems. A programmer targetting a single country might make the service available under more than one system if that country was effectively supporting more than one conditional access standard.

Before such a path could be implemented, considerable systems analysis and software development would be required to ensure that the access control mechanisms of one system can be adequately mapped to those of another. To take a simple example, both Eurocypher and EuroCrypt-M [EC89] possess programme rating schemes, but EuroCrypt-M only allows definition of a single rating level, normally related to the point of transmission, while Eurocypher allows definition of different ratings in different reception regions, as well as ratings based on programme content. The programmer must make a choice whether to operate within the limits set by the facilities which are common to two systems, or whether to operate the two systems independently of each other.

Multiple conditional access system operation is currently only an option in MAC-based systems, since only MAC possesses an SI capability. In order to allow similar features to work in PAL-based systems, the PAL equivalent of certain portions of SI are required. Currently, the only path to preventing market fragmentation of PAL-based subscription services on technological lines is to build a multiple standard PAL receiver, in which the user selects the conditional access system required for each channel change.

4 Summary

BSB now have in place fully operational customer management and Eurocypher conditional access systems. The systems architecture outlined above provides for sophisticated control and reliable operation of a conditional access subscription television service. It provides all the functions and features required to support the continued operation and growth of BSB for the future. The Eurocypher systems are capable of being configured in ways which allow support for many programmers in complex multinational environments, and with the provision of appropriate data collection systems can also support additional features such as Impulse Pay Per View.

5 References

[Bennett90] - C. J. Bennett, P. Moroney, D. J. Cutts: The Architecture and Security Goals of the Eurocypher System. Proc ACSA90, June 1990 (This conference)

[EC89] - "Systeme D'Access Conditionel pour La Famille MAC/Pacquet: Eurocrypt" Paris, March 1989

CARACTÉRISTIQUES FONCTIONNELLES D'UN GESTIONNAIRE DES TITRES D'ACCÈS ET D'UN SYSTÈME DE GESTION COMMERCIALE

Philippe SALANOVA
TÉLÉSYSTÈMES
Division Réseaux et Communication
L'Equerre
315 rue Hélène Boucher
78280 GUYANCOURT
FRANCE
Tél : +33 30 96 40 37

TABLE DES MATIÈRES

1.1 INTRODUCTION

Dans le cadre du développement des services de télévision à condition d'accès, FRANCE TELECOM a lancé un programme qui met en oeuvre les élèments fonctionnels suivants :

- un centre de gestion

- un dispositif d'embrouillage des signaux audiovisuels avant leur diffusion

- un terminal de désembrouillage destiné à restituer en clair les signaux reçus, chez les usagers autorisés. Ce terminal a pour nom le VISIOPASS.

Le service VISIOPASS est adapté à l'évolution vers la télévision à haute définition. Ce service permettra entre autre à l'abonné de ne payer que les émissions qu'il désire regarder.

TELESYSTEMES a été retenu par FRANCE TELECOM pour la réalisation du centre de gestion. Ce dernier se compose de deux systèmes :

- Un gestionnaire des titres d'accès (GTA) qui assure entre autre la gestion de cartes à mémoire de technologie PC2 (support des titres d'accès) et la mise à disposition de ces titres d'accès aux usagers. Il est prestataire de service pour tous les systèmes de gestion commerciale.

- Un système de gestion commerciale (SGC) qui organise l'offre commerciale de FRANCE TELECOM pour le compte des fournisseurs de programme, la présente aux usagers via un serveur vidéotex et gére aussi la vente des émissions des différentes chaines aux abonnés du service VISIOPASS.

Ces deux systèmes GTA et SGC sont réalisés par la Division Réseaux et Communication de TELESYSTEMES Télécommunication sur la gamme CLX 700 de TANDEM (machines à tolérance de panne).

1.2 PRINCIPE

Contrôler l'accès à des services audiovisuels, diffusés indépendamment du réseau de diffusion (réseaux vidéocommunications, satellite).

Proposer des lots de programmes audiovisuels en mode abonnement, ou achat anticipé et, dans une deuxième étape, un service à la carte.

Facturer la prestation à l'usager et rémunérer des fournisseurs.

L'autorisation d'accès à un service est matérialisée par la possession d'un titre d'accès sur le support carte à mémoire PC2.

1.3 COMPOSANTES

- Des émetteurs, des récepteurs, des lots de programmes appelés PAC

- Un dispositif d'embrouillage : les points d'embrouillage

- Un dispositif de désembrouillage: le terminal Visiopass et la carte PC2, chez l'usager

- Un dispositif de contrôle d'accès ou péage : le GTA (Gestionnaire des Titres d'Accès)

- Un dispositif de gestion : le SGC (Système de Gestion Commerciale)

1.4 DESCRIPTION DE L'ENVIRONNEMENT DU GTA ET DU SGC

L'outil d'émission des cartes chargé d'initialiser les cartes vierges en provenance des fabricants. Il reçoit ses ordres du GTA (sous forme de scénario d'émission) et lui communique un compte rendu d'exécution lorsque l'émission des cartes est terminée.

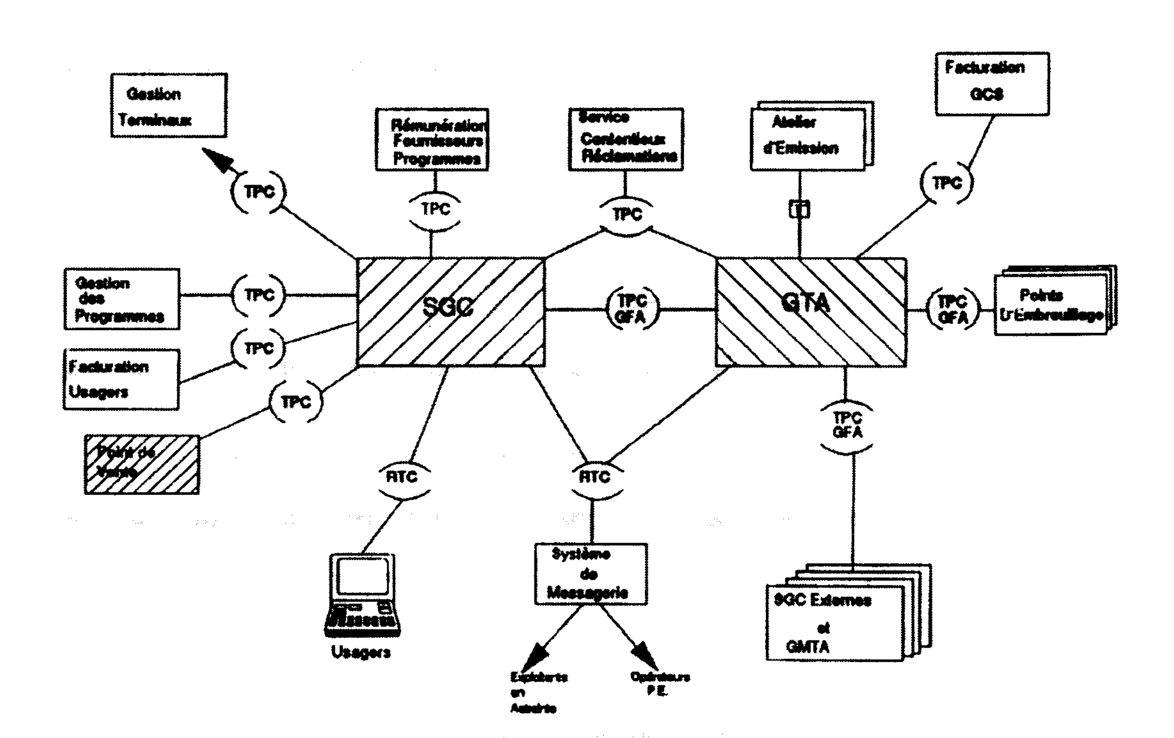
Des systèmes de gestion commerciale propres aux fournisseurs de programmes ayant pour fonctions principales, la gestion de ces fournisseurs, l'élaboration de leurs caractéristiques de commercialisation, la gestion des usagers et des cartes. Un système de gestion commerciale est sous la responsabilité d'un gérant commercial de services. (GCS).

Des points d'embrouillage (PE) qui ont pour principale mission de fournir un signal codé et embrouillé ; ils assurent le transport des titres d'accès vers l'usager. Le GTA communique avec les PE par l'intermédiaire des diffuseurs de messagerie.

Des terminaux VISIOPASS (désembrouilleurs) qui utilisent la carte PC2 de l'usager pour analyser les messages de gestion et contrôler les autorisations de désembrouillage.

Le centre de facturation des gérants commerciaux de services qui émet et gère les factures à destination des utilisateurs des services offerts par le GTA.

Graphique de l'environnement du Centre de gestion



2. LE GTA

2.1 PRESENTATION

. Le but du système d'accès conditionnel EUROCRYPT est de contrôler l'accès à des services audiovisuels diffusés, sur tout réseau de vidéo-communications ou satellite : il faut s'assurer que des programmes de télévision, de radio ou des services de données ne sont accessibles qu'aux seuls usagers qui remplissent des conditions bien précises, par exemple avoir souscrit un abonnement.

. Le système est composé de trois équipements : le gestionnaire des titres d'accès (GTA), le système de gestion commerciale (SGC), et les terminaux points de vente (TPV).

. Le GTA remplit les fonctions de gestion technique relevant de l'autorité émettrice pour des systèmes de gestion commerciale.

. Le GTA a un rôle de prestataire de service d'accès conditionnel vis à vis de ces fournisseurs. L'une de ses fonctions est donc de contrôler ces fournisseurs et de fournir les éléments de facturation du service rendu.

. Le GTA intervient pour la gestion des cartes (supports des titres d'accès), la mise à disposition des titres d'accès aux usagers via les points d'embrouillage ou les terminaux points de vente et les relevés d'achats d'émission.

. Les différents modes d'accès offerts par le système d'accès conditionnel sont les suivants :

- abonnement simple
- abonnement par thème/niveau
- abonnement par classes
- achat anticipé à la séance
- achat impulsif à la séance
- achat impulsif à la durée

L'achat impulsif à la durée nécessite en particulier la version EEPROM de la carte PC 2 qui permet l'effacement d'informations sur la carte. Une carte EPROM serait très rapidement saturée.

2.2 FONCTIONS

Les fonctions assurées sont les suivantes :

Saisir et maintenir les informations de configuration

Saisir et maintenir les informations "émetteur"

Saisir et maintenir les informations sur les Gérants Commerciaux de Services et leurs entités service.

Fournir les élèments de facturation du service fourni par le GTA

Gérer l'émission des cartes

Gérer les cartes mères

Gérer les clés

Gérer les adresses

Gérer les cartes usager

Elaborer et traiter les messages de gestion (EMM)

Gérer la relation avec les SGC et GMTA

Traiter les requêtes en provenance des SGC et GMTA

Gérer les PAC

Effectuer les relevés des consommations en mode impulsif

Gérer l'effacement d'informations sur les cartes

Gérer la relation avec les points d'émission

2.3 ORGANISATION DU GTA

Le GTA est sous la responsabilité de l'Administrateur du GTA qui dispose des droits d'accès sur l'ensemble du GTA.

Il est entouré d'une équipe "d'opérateurs du GTA" à laquelle il délègue un certain nombre de tâches.

Leur rôle est de :

- Maintenir l'environnement du GTA.

- gérer les paramètres qui les concernent directement : points d'embrouillage, canaux, émetteur, accès au système.

- gérer les paramètres des GCS en accord avec ceux ci, en s'assurant que l'ensemble reste cohérent : entités services, modèles d'émission cartes, diffusion de message.

- Gérer l'émission des cartes, effectuer le suivi avec les ateliers d'émission, la tenue de stocks de cartes vierges.

- L'exploitant du système à la charge , sur la console du système TANDEM, de superviser les traitements du GTA.

Son rôle est de :

- gérer l'actitité quotidienne du système

- planifier les traitements à la demande

- analyser et gérer les incidents

- consulter et utiliser les procédures de test et de contrôle du système

- contrôler la bonne exécution des traitements, en diffuser les résultats

- gérer l'environnement matériel et les consommables

- assurer les relations avec les services de maintenance

2.4 MODE D'EMPLOI DU GTA POUR UN GCS

Les services GTA accessibles à un GCS font l'objet d'un contrat entre ces deux parties.

L'accès au GTA se fait par 2 moyens :

- manuels — Courrier, télex, etc. [demande de cartes, maintenance des données propres au GCS]

- automatiques — Requêtes transmises par la liaison de données SGC - GTA [ordres de gestion cartes,...]

2.5 LA SECURITE DANS LE GTA

La sécurité dans le GTA consiste à traiter des EMM envoyés par l'applicatif. Ce traitement consiste à chiffrer ou à signer des parties d'EMM.

La sécurité dans le GTA est assurée par des processeurs de sécurité appelés UDS/PC2 (Unité Décentralisée de Sécurité pour les cartes PC2)

L'UDS/PC2 est basée sur un compatible PC sous MS/DOS sur lequel sont connectés des lecteurs de cartes à mémoire.

Ils sont connectés au GTA par des liaisons directes X25 à 19200 bauds.

Leur interface avec l'applicatif GTA sont des process appelés moniteur des GUDS/PC2 (Gestionnaire Unité Décentralisée de sécurite pour les cartes PC2).

Il y a un GUDS/PC2 par UDS/PC2. Ils sont supervisés par un moniteur qui effectue le partage de charge entre eux.

Les process qui veulent effectuer des opérations de chiffrement ou de signature d'EMM transmettent au GUDS/PC2 des messages contenant les requêtes à traiter.

Sur chaque UDS/PC2 sont connectés 4 lecteurs de carte à mémoire destinés à recevoir des cartes mères de type PC2. La fonction de sécurité principale de l'UDS/PC2 est de faire calculer les cartes PC2 enfichées dans les lecteurs.

Les transferts d'informations entre le système hôte et l'UDS/PC2 doivent être minimisés afin d'éviter une surcharge de l'UC du site central. Le maximum de traitement doit donc être effectué par l'UDS/PC2 (découpage d'EMM et formatage du résultat) et les cartes, afin de décharger le central.

L'UDS/PC2 reçoit des requêtes du GTA via le GUDS/PC2. Il analyse le contenu de l'EMM reçu, envoie des ordres à une carte qu'il aura sélectionnée. Lorsque le calcul est terminé, il reconstitue l'EMM l'envoie au GUDS/PC2 qui remonte l'EMM traité à l'applicatif.

Les principales fonctions exécutées par les cartes PC2 sont le chiffrement et la signature des EMM. En effet, tout ordre d'écriture reçu par une carte fille ne sera exécuté que s'il a été préalablement signé par une carte mère valide.

D'autre part, les calculs de chiffrement ou de signature des cartes mères, sont faits en utilisant un paramètre identifiant de façon unique la carte fille destinatrice (ce paramètre est appelé le diversifiant).

De ce fait aucune autre carte fille que celle concernée ne pourra interpréter un ordre. Ceci permet d'éviter qu'un EMM transmis ne soit intercepté et présenté à une autre carte.

Le GUDS/PC2 étant installé sur une machine de type NON STOP, ceci assure une sécurité de fonctionnement élevée. D'autre part les UDS/PC2 sont doublés, ce qui permet un partage de charge au niveau des requêtes émises par les GUDS/PC2 ainsi qu'une continuité de fonctionnement en cas de panne d'un des PC.

Le GTA gère donc ,via le moniteur des GUDS/PC2, deux UDS/PC2 soit 8 cartes PC2 . Ceci permet de supporter la charge des requêtes demandées au GTA.

Les lecteurs de cartes et les cartes sont gérés en "pool", ce qui permet un partage de la charge et une continuité de fonctionnement en cas de défaillance d'un composant.

Afin de détecter d'éventuelles pannes sur les lecteurs ou sur les cartes, des programmes de test peuvent être activés de façon manuelle ou automatique. Ces tests sont effectués pendant les périodes où les cartes ne sont pas en train de calculer pour le GTA. En cas de résultat négatif sur un test de lecteur ou de carte , le résultat est remonté à l'applicatif du GTA qui décide des actions à entreprendre (affichage console ou autre , alarme..)

Comme indiqué plus haut , chaque UDS est connecté par une liaison directe en X25. Deux circuits virtuels par UDS/PC2 permettent le dialogue entre l'UDS/PC2 et le GUDS/PC2. Un circuit est utilisé pour l'émission de messages à destination de l'UDS/PC2 ; l'autre étant utilisé pour la réception de messages en provenance de ce dernier.

D'autre part sur chacun des liens, le GUDS multiplexe les requêtes à destination ou en provenance des UDS/PC2.

2.6 DESCRIPTION DE LA CONFIGURATION MATERIELLE

1 système TANDEM CLX 700 configuration 2 processeurs comprenant :

- 2 processeurs CLX 700 avec 16 M0 de mémoire chacun
- 4 disques 300 M0 mirorisés (soit 2 disques logiques)
- 6 disques 300 M0 mirorisés (soit 3 disques logiques)
- 3 terminaux à écran
- 1 imprimante série 400 cps
- 2 contrôleurs de communication
- 1 dérouleur de bande 1600 BPI

2 Unités de Sécurité modèle 500 pour cartes mères PC2 comprenant :

- 1 UC 286
- 20 M0 de disque
- 1 carte X25
- 1 carte multivoies asynchrones

1 coffret de sécurité pour cartes mères PC2 comprenant :

- 8 lecteurs reliés par 8 E/S série à 19200 bps.

1 PC 386 pour les statistiques et pour toutes les interfaces disquette avec l'outil d'émission comprenant :

- 2 M0 de RAM
- 140 M0 disque
- 1 imprimante graphique
- 1 carte Safe-card permettant un accès sécurisé sur PC

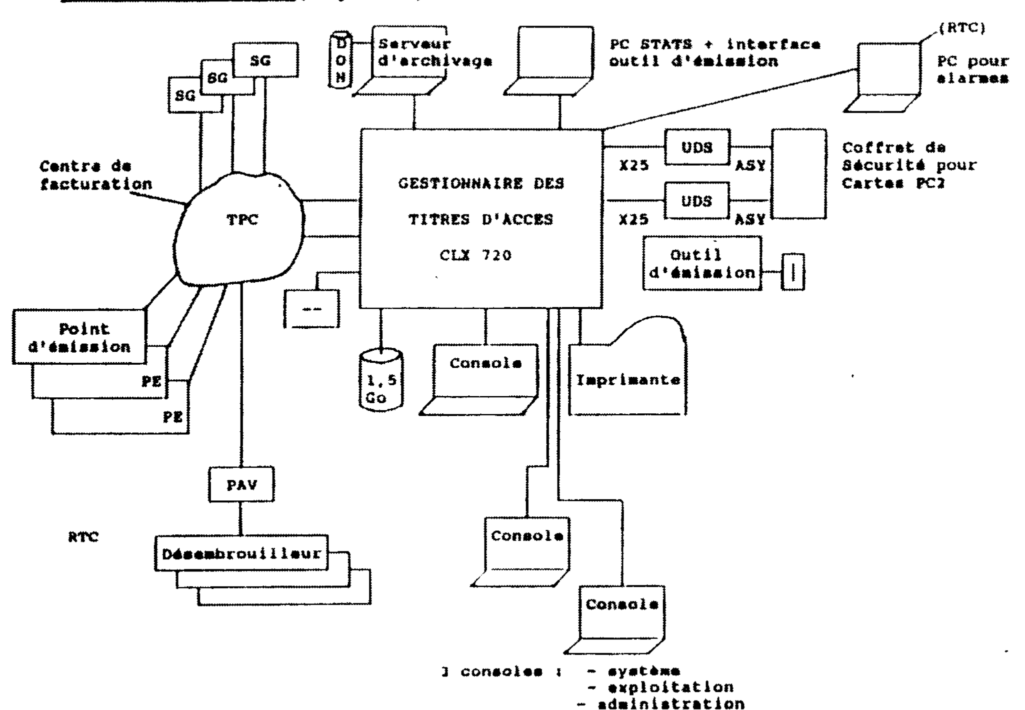
1 PC 386 pour la gestion des alarmes

- 40 Mo disque
- 1 carte Safecard permettant un accès sécurisé sur PC
- 1 carte ASP-440 version X32 permettant la connexion à ATLAS 440
- 1 carte numéroteur avec son modem incorporé

1 serveur d'archivage comprenant :

- 1 UC 80386, 16 MHz, 1 M0
- 1 disque dur 40 M0
- 1 DON 1G0
- 1 carte Safe-card permettant un accès sécurisé sur PC

Schéma de la configuration matérielle (configuration site)



3. LE SGC

3.1 PRESENTATION

Dans le système d'accès conditionnel, il y a plusieurs SGC. Ici, nous ne décrirons que celui de France Télécom. Il existe d'autres SGC dont les fonctionnalités sont libres; la seule contrainte étant le respect du protocole "Interface SGC-GTA".

Le SGC est responsable de l'offre commerciale du système d'accès conditionnel.

A ce titre, il est en relation avec :

- les fournisseurs, qui définissent l'offre commerciale et la programmation

- les points de vente, à qui il délègue la distribution des produits

- les usagers (avec accès à un serveur VIDEOTEX), par l'intermédiaire de la relation avec les points de vente et la facturation des produits (PAC)

Le Gérant Commercial des Services (GCS) est l'unique responsable du SGC.

Il négocie avec le GTA un contrat définissant les choix du SGC vis à vis du GTA.

Il négocie avec les fournisseurs des contrats permettant de définir l'offre commerciale du SGC.

Il négocie des contrats avec les responsables des points de vente qui permettront ensuite au SGC de commercialiser ses PAC.

Il commercialise certains types de carte à mémoire (PC2). Il est l'autorité émettrice de ces cartes mais après négociation avec les GCS des SGC externes il peut autoriser l'utilisation de ces cartes par des clients de ces SGC externes. Pour cela, il leur alloue une ou plusieurs zones de service dans la carte. Il peut également négocier avec d'autres GCS l'utilisation pour les clients du SGC de France Télécom de certaines des cartes de ces GCS.

Il commercialise les terminaux Visiopass, qui, avec la carte PC2 contenant les titres d'accès, permet le désembrouillage des émissions.

Les programmes audiovisuels sont commercialisés sous forme de PAC pouvant regrouper plusieurs programmes, avec différents modes d'accès.

Les différents modes d'accès offerts par le système d'accès conditionnel sont les suivants :

- abonnement simple

- abonnement par thème/niveau

- abonnement par classes

- achat anticipé à la séance

- achat impulsif à la séance

- achat impulsif à la durée.

3.2 FONCTIONS

On peut recenser sept grandes fonctions assurées par le SGC, à savoir :

Fonction commerciale de présentation, promotion et distribution des PAC

Fonction de gestion de programmes

Fonction de gestion de stocks et de distribution des cartes et des terminaux

Fonction de facturation et de rémunération

Fonction d'interface avec le GTA (Gestionnaire des Titres d'Accès : responsable technique du Système à Accès Conditionnel)

Fonction de gestion des contentieux

Fonction de statistiques

Ces fonctions correspondent aux gestions et relations suivantes :

- Gérer les fournisseurs de programmes audiovisuels utilisateurs du système de gestion commerciale

- Prendre en compte les caractéristiques des programmes audiovisuels offerts par chaque fournisseur.

- Gérer les points de vente

- Gérer les usagers des services audiovisuels

- Gérer la relation avec les points de vente

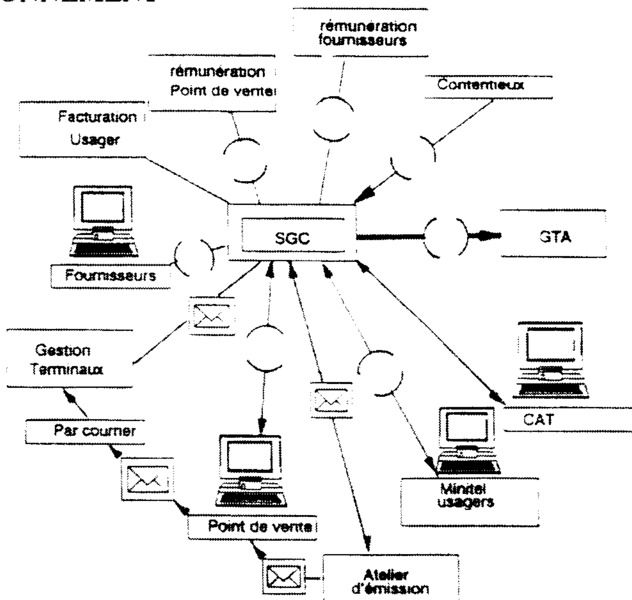
- Offrir une relation "usager - SGC" via un serveur vidéotex

- Offrir une relation "usager - SGC" via un centre d'opérateurs

- Elaborer les requêtes à destination du GTA

- Disposer d'interfaces avec l'exploitant du SGC

3.3 ENVIRONNEMENT



Sont connectés au SGC:

- Le GTA, via Transpac (en mode GFA - groupement fermé d'abonnés)

- Les usagers, par

  . leur minitel
  . les consoles Tandem du CAT (centre d'appel téléphonique), pilotées, par téléphone, par les usagers

- Les points de vente, appelés TPV

- Les fournisseurs par Minitel

- Les Centres Comptables, à savoir :

  . le centre de facturation des usagers
  . le centre de rémunération des fournisseurs de programmes
  . le centre de rémunération des points de vente

Ces Centres peuvent être distincts ou confondus.

- Le service contentieux

La relation de ces Centres avec le SGC est réalisée par transfert de fichiers, avec repli sur bande magnétique .

- L'atelier d'émission qui livre les lots de cartes au SGC et aux points de vente, mais le SGC et le TPV ne connaissent pas ce centre

- Le centre de gestion des terminaux qui livre des lots de terminaux suite à des commandes envoyées par le SGC

3.4 L'USAGER ET LE SGC

L'usager doit avant toute opération établir un contrat. Pour ce faire il se rend à un point de vente (la liste des points de vente est disponible sous minitel).

A ce point de vente l'usager signe un contrat contenant des informations d'identité, de mode de paiement, de réseau de diffusion, de liste de cartes et terminaux ainsi que de lieu d'achat et de mise en opposition (TPV, CAT ou minitel).

L'usager d'un réseau non desservi par le SGC est averti avant la conclusion du contrat.

Avec son contrat l'usager reçoit les cartes et les terminaux qu'il a demandé, et en contre-partie il règle au TPV une caution.

L'usager abonné va ensuite pouvoir bénéficier de certains services qu'il pourra obtenir au TPV, au CAT ou par minitel dans la mesure où son contrat le permet.

Le numéro de contrat est nécessaire pour l'accès de la majorité des services. Par ailleurs, le numéro de contrat est rappelé pour chaque facturation.

Si l'usager perd son contrat papier il retourne à un point de vente avec une de ses cartes pour obtenir un duplicata du contrat. Le point de vente pouvant accèder aux contrats par un nom d'abonné, lorsqu'une carte de cet abonné est dans le lecteur de carte du Point du Vente (LECAM).

Pour toutes modifications de son contrat (retour ou nouvelle demande de cartes ou de terminaux, changement d'adresse, de coordonnées bancaires) l'usager se rend obligatoirement à un point de vente.

L'usager qui fait un achat le fait pour toutes les cartes liées à son contrat, sinon il ouvre plusieurs contrats.

L'usager qui a plusieurs résidences ouvre plusieurs contrats.

La facturation est mensuelle pour l'abonnement, totale pour l'anticipé fonction de la quantité achetée, de la durée d'abonnement et des incidents de diffusion ou de déprogrammation dans la mesure ou le fournisseur l'accepte.

L'usager qui ne consomme pas (aucun achat, aucun droit à la période de facturation) et qui ne loue aucun terminal se voit facturer des frais de gestion.

L'usager qui loue des terminaux paie une redevance mensuelle.

Aucun autre service ne sera facturé.

Pour se désabonner l'usager doit avant l'échéance de son abonnement informer le SGC de sa volonté, sinon l'abonnement est automatiquement reconduit pour la même durée. Il ne peut se désabonner avant l'échéance, il recevra une facture jusqu'à l'échéance de son abonnement.

En cas d'incidents de paiement , le centre de facturation peut geler ou résilier le contrat de l'usager.

3.5 LE FOURNISSEUR ET LE SGC

Le Fournisseur établit un contrat avec le GCS qui lui fournit deux authentifieurs.

Des éléments de contrats sont introduits par l'exploitant du SGC.

Ces contrats précisent l'identification du fournisseur, les identificateurs de service utilisés, les chaines commercialisées (et les caractéristiques réseaux de ces chaines), le nombre maximum de PAC commercialisés et leur types , les critères de rémunération (le fournisseur ne peut pas définir plus de 10 chaines).

Le GCS a fourni au fournisseur la liste de modèles de diffusion et la plage des numéros de séances utilisables.

Les opérations effectuées par le fournisseur le sont sous contrôle de l'authentifieur :

- création, modification, suppression de PAC

- mise à jour des grilles de programmes (connues deux semaines maximum à l'avance) et introduction de pages de textes libres.

- mise à jour du descriptif de chaines.

Périodiquement le fournisseur est rémunéré à partir des éléments fournis par le SGC à date définie par le GCS.

La suppression d'un fournisseur ne sera effective que lorsqu'il n'y aura plus de PAC (périmés ou sans destinataires) et que tous les éléments financiers seront totalement traités.

Le fournisseur doit définir les données EUROCRYPT (n° de séance, thème), associer au numéro de PAC un libellé, définir son offre dans un "texte libre" et définir une partie financière.

Cette partie financière permet de donner :

- des coûts en fonction du nombre d'exemplaires achetés

- des coûts en fonction de la durée de l'abonnement : cette tarification n'est modifiable que trois fois par an.

- l'autorisation d'effectuer des dégrèvements en cas d'incidents ou de déprogrammation.

- des durées mini et maxi d'abonnements. On garantit à l'usager un tarif stable pendant toute la durée de l'abonnement.

- des dégrèvements pour des achats de PAC anticipé si certaines séances sont déjà écoulées.

Les PAC abonnement sont à renouvellement automatique géré par le GTA par période de 1 mois. Ils sont facturés au mois aux usagers. Les PAC anticipés à la séance sont totalement facturés à l'usager à la période de facturation qui suit achat.

La modification d'un PAC ne peut porter sur les zones liées aux titres d'accès.

Le fournisseur peut supprimer des PAC, mais les PAC périmés sont automatiquement supprimés par le GTA.

3.6 LE POINT DE VENTE ET LE SGC

Le TPV établit un contrat avec le GCS et, s'il décide de gérer ses stocks il reçoit des stocks de cartes et terminaux.

Il reçoit dans tous les cas 2 AV.

Par contrat il définit :

- ses stocks max et mini (s'il en gère)

- son type de rémunération.

Des éléments du contrat sont introduits au SGC par l'exploitant du SGC ou par minitel équipé d'un AV maitre.

Tous les transferts de matériel (cartes, terminaux) se font obligatoirement au TPV et entre autres :

- les cartes rendues ne sont pas recyclées.

- les terminaux hors service sont envoyés à des centres de réparation . Cette fonction n'est pas vu par le SGC qui se contente de constater une diminution du stock.

- les cartes retenues par l'usager qui sont la contre-partie d'une caution conservée par le TPV avant d'être transmise à France Télécom.

- les terminaux retenus par l'usager qui sont la contre-partie d'une caution conservée par le TPV avant d'être transmise à France Télécom. Lors d'un échange de terminaux aucune caution n'est perçue et le SGC se charge d'en informer le centre de facturation des delta de caution à rendre ou à percevoir.

Le point de vente peut également encaisser à la place de France Télécom, le paiement des factures usagers dans le cas où le contrat de l'usager a été suspendu. Le vendeur doit en informer le SGC (RHM de paiement, RHM de modification de contrat).

Le vendeur du TPV a une fonction de conseil vis-à-vis de l'usager : le vendeur maitrise bien l'environnement VISIOPASS.

Le TPV est rémunéré au forfait ou à l'activité en fonction du nombre de contrats ouverts et du nombre de cartes.

Les modifications du contrat portent sur les stocks et le type de rémunération. Ces modifications sont introduites par un exploitant du SGC ou un utilisateur d'un Minitel équipé d'un AV maitre.

La suppression du TPV ne peut être faite que par un exploitant du SGC. Elle n'est effective que lorsque les cartes et les terminaux ont été renvoyés au SGC et lorsque les éléments de rémunérations ont tous été traités.

3.7 LE CAT ET LE SGC

Le CAT ou Centre d'Opérateurs permet aux usagers d'accéder aux fonctions commerciales par l'intermédiaire d'opérateurs en liaison téléphonique avec l'usager .

Les prestations offertes couvrent les domaines suivants :

- présentation des services offerts (rubrique d'informations générales).

- mode d'emploi du service et du terminal.

- fourniture d'annuaires.

- accès aux grilles de programmes.

- prise en compte des réclamations.

- rubrique Mini-Point de Vente, qui est en fonction optionnelle pour usager, car outre la possibilité de présentation d'informations individuelles sur un usager donné, il est laissé libre choix à celui-ci de :

. demander la mise en opposition par appel du CAT

. acheter ses titres d'accès par le CAT.

3.8 DESCRIPTION DE LA CONFIGURATION MATERIELLE

- 1 système TANDEM CLX700 configuration 4 processeurs comprenant :

. 4 processeurs CLX 700 avec 12 M0 de mémoire chacun

- 6 disques 300 M0 mirorisés (soit 3 disques logiques)
- 1 imprimante série 400 cps
- 2 contrôleurs de communication
- 1 dérouleur de bande 1600 BPI
- 25 terminaux à écran

- 2 unités de Sécurité modèle 500 comprenant :

  - 1 UC 286
  - 20 M0 de disque
  - 1 carte X25
  - 1 carte additionnelle DES

- 1 PC 386 pour les statistiques et pour les interfaces disquette comprenant :

  - 2 M0 de RAM
  - 140 M0 disque
  - 1 imprimante graphique
  - 1 carte Safe-card permettant un accès sécurisé sur PC

- 1 PC 386 pour la gestion des alarmes

  - 40 M0 disque
  - 1 carte Safe-Card permettant un accès sécurisé sur PC
  - 1 carte ASP-440 version X32 permettant la connexion à ATLAS 440
  - 1 carte numéroteur avec son modem incorporé

- 1 serveur d'archivage comprenant :

  - 1 UC 80386, 16 MHz, 1 M0
  - 1 disque dur 40 M0
  - 1 DON 1G0
  - 1 carte Safe-card permettant un accès sécurisé sur PC

Schéma de la configuration matérielle (configuration site)

LECAM
Minitel TPV
Centre de facturation et rémunération fournisseurs
DON
Serveur d'archivage
PC STATS
(RTC)
PC pour alarmes
UDS
X25
UDS
X25
SYSTEME DE GESTION CLX 740
--
TPC
RTC
P
A
V
GTA
900 Mo
Console système
Imprimante
Minitel usager
Minitel fournisseur de programme
Console
Console

25 terminaux
└> Référence 6526A

3 consoles : - système
- exploitation
- administration

4. GLOSSAIRE

AV	Authentifieur Vidéotex
CAT	Centre d'Appel téléphonique
DM	diffuseur de messagerie
ECM	Message contrôle des titres d'accès (ECM = Entitlement Checking Message)
EMM	entitlement management messages (message de gestion)
EEPROM	Technologie de composant à mémoire programmable et effaçable électriquement (EEPROM = Electrically Erasable Programmable ROM)
EPROM	Technologie de composant à mémoire programmable électriquement et effaçable par rayons UV (EPROM = Electrically Programmable ROM)
EUROCRYPT	Nom du système d'accès conditonnel dont les processeurs de sécurité sont des cartes à mémoire de type "Porte clés".
GCS	Gérant commercial de service
GTA	Gestionnaire des titres d'accès
LECAM	Lecteur de carte à mémoire
GUDS	Gestionnaire d'Unité Décentralisée de Sécurité.
PAC	Produit Audiovisuel Commercialisé : offre commerciale faite aux abonnés.
PC2	Porte clefs numéro 2 - nom donné à la carte
PE	point d'embrouillage
SGC	Système de gestion commerciale
TPV	Terminal point de vente

MANAGING SMART CARDS FOR PAY TELEVISION

THE VIDEOCRYPT™ APPROACH

Jonathan **HASHKES**, Michael **COHEN**
News Datacom
PO BOX 1763
JERUSALEM
ISRAEL
Tél : +972 2 240545

ABSTRACT

VideoCrypt™, a joint project of News Datacom and Thomson Consumer Electronics, incorporates a detachable, smart-card system for controlling access to pay television services. The system provides two primary ways for managing these smart cards : (1) over-the-air addressing of currently installed cards and (2) card remplacement. The paper presents an overview of the VideoCrypt™ approach to pay-TV security, a description of the system, and a review of the tools and methods provided for managing smart cards.

RÉSUMÉ

VideoCrypt™, projet commun de News Datacom et Thomson Consumer Electronics, comprend un système de contrôle d'accès détachable basé sur la carte à puce pour les services de télévision à péage. Le système offre deux possibilités de gestion de ces cartes : (1) l'adressage sur antenne de cartes utilisées actuellement et, (2) le remplacement de la carte. L'article présente une vue générale de l'approche VideoCrypt™ pour la sécurité en télévision à péage, une description du système et un examen des outils et des méthodes fournies pour la gestion des cartes.

TABLE OF CONTENTS

1. Piracy: Enemy No. 1 of the Pay TV Industry

According to a report of the U.S. Federal Communications Commission, the number one problem facing the Home Satellite Dish industry today is theft of satellite program services (so-called 'piracy'). Industry experts estimate that at least 50 percent of all decoders in use are "pirate boxes".[1] Theft of service equally haunts the cable-TV industry.

These facts arise against a background of repeated claims of "unbreakable security" by the developers of existing television security systems. Each of the claims has been proven false. At least one company has even promoted its "fully secure" system as an industry standard. That system, too, has been broken.

In conventional systems, the user's decoding key resides in the decoder. When pirates crack the code, the security of the system is compromised. System security can be restored only by replacing each subscriber's decoder—a prohibitively expensive solution. In addition, the decoder's initial design permanently determines system features, which can only be altered by a similar system-wide replacement of decoders.

2. The VideoCrypt™ Answer

VideoCrypt™, a joint development of News Datacom and Thomson Consumer Electronics, incorporates a *detachable* access-control system for pay television. *Detachable*, because its security secrets and algorithms reside solely in inexpensive and easily replaceable smart cards. It is, therefore, the first system that gives pay TV service providers not only top security, but which is also endlessly adaptable and easy to manage.

VideoCrypt™ makes these claims based on its unique approach to television broadcast security. Its flexible design derives from the following premises:

- Technology for television security will continue to advance.
- Fixed security algorithms are not secure in the long run.

Encoding and decoding equipment must, therefore, incorporate a flexible security system that can both adapt to changes in video-scrambling technology and provide new security algorithms, as needed.

With VideoCrypt™, there is no need to choose a fixed standard. More powerful security algorithms can be developed as stronger smart card microprocessors become available at lower cost. Hence, while pirates can be expected to use increasingly sophisticated methods to break the algorithms, VideoCrypt™ will always stay several steps ahead.

---

[1]*FCC 89-104: Notice of Inquiry* (Washington, D.C.: Federal Communications Commission, April 1989), 2

3. The Smart Card

VideoCrypt™ achieves these breakthroughs with a revolutionary application of smart card technology. All entitlements and authorization keys reside on the smart card (a card, resembling a credit card, that contains a computer microchip). The generic decoder holds no secrets. The decoder's only security-related function is to continuously verify the legitimacy of the smart card—called "Fiat-Shamir zero-knowledge authentication." All the other security aspects are managed by the smart card.

The microprocessor in the smart card employs innovative public key security techniques. To access pay television channels, a changeable security algorithm instructs the decoder how to rearrange the scrambled video.

Replacement smart cards are inexpensive and can be sent to each subscriber either periodically (e.g., every three months) or whenever there is reason to believe that system security has been breached. With each batch of new cards, security algorithms and entitlement types can be changed. Unauthorized attacks on security are, therefore, extremely difficult to mount and economically not viable.

Moreover, smart cards have applications beyond the security realm. As a business tool, they can be used for: advertising, promotional marketing, TV merchandising, and payment reminders.

4. How VideoCrypt™ Works

The VideoCrypt™ system is applicable to any signal type (PAL, SECAM, NTSC, MAC, D2-MAC) and to any signal medium (cable, terrestrial, satellite). It is most effective when combined with a "hard" scrambled video signal (such as video line rotation), and can also be used with many types of scrambled audio signals.

The smart card serves as an *active security device*, which manages the scrambling/descrambling process and dictates overall system behavior. In contrast, in other smart-card–based systems, the smart card is passive, used only as a repository of keys. The decoder is still limited to its fixed scrambling algorithm and original system features. It is the active nature of the VideoCrypt™ smart card that makes VideoCrypt™ unique.

The scrambling/descrambling process begins in the broadcasting studio, where every 0.6 to 2.5 seconds, the Security Encoder Computer sends a packet of control data to its smart card. In response, the smart card generates a random scrambling "seed" using a VideoCrypt™ security algorithm.

The seed, together with control data and selected subscriber and scheduling information, is passed to an encoder. The encoder uses the seed to scramble the video before transmission. The control data and subscriber/scheduling information is transmitted over the air with the scrambled television signal.

At the receiving end, the control data is routed by the decoder to the viewer's smart card. The smart card "hashes" together the data using the appropriate security algorithm and produces a seed (identical to the seed used to scramble the picture at the broadcasting studio). The seed is sent back to the decoder, where it is used to reconstruct (i.e., descramble) the video picture.

The control data also triggers the smart card to authorize individually addressed actions, including: enabling/disabling of entitlements, payment reminders, and personal messages.

5. The System

The VideoCrypt™ system includes four major components (*see Figure 1*).

5.1 Subscriber Management System

The Subscriber Management System handles all subscriber-related information, including: orders for regular service, "booking" for pay-per-view programs, orders for service upgrades (or downgrades), cancellations, billing details, and payment histories. It notifies the Authorization Center of entitlements to be modified, messages to be broadcast (e.g., payment reminder) and cards to be "blacklisted". It is also responsible for relaying all necessary instructions for the production of smart cards. (*See also Section 6, "Smart Card Management."*)

5.2 Authorization Center

The Authorization Center computers manage the generation of scrambling seeds and the preparation of information from the Subscriber Management System and program scheduling computers for transmission. It sends this information to the Encoder.

5.3 Encoder

The Encoder scrambles the video signal according to the seed received from the Authorization Center. It transmits the scrambled signal together with subscription and program information.

5.4 Decoder

The broadcast transmission is received by the decoder and the control data is forwarded to the smart card. The smart card "hashes" the data to create the appropriate seed. It then transfers the seed back to the decoder, where it is used to descramble the video picture.

6. Smart Card Management

There are two primary elements in VideoCrypt™ smart card management:

- Over-the-air addressing
- Card replacement

Both of these activities are initiated from the Subscriber Management System.

6.1 Functions of the Subscriber Management System

The Subscriber Management System is the comprehensive customer information database for the VideoCrypt™ pay-TV scrambling and security system. Developed by News Datacom using the fourth-generation database applications environment, MAGIC, its main functions include (*see Figure 2*):

- **Customer Service** - The Subscriber Management System enables rapid on-line retrieval of all information about a customer, including: subscriptions, method of payment, account history, smart card data. It also provides the tools needed to enter new information and modify existing records.

- **Billing and Accounting** - The Subscriber Management System handles all aspects of customer billing. Its banking interface handles the transfer of claim and payment information to and from the banks and credit card companies. An extensive reporting facility facilitates effective auditing of network operations.

- **Initiation of Over-the-Air Addressing** - The Subscriber Management System data is used to regulate subscriber privileges and guarantee system security. It generates orders to enable and disable viewing entitlements, broadcast on-screen payment reminders, send letters to customers delinquent in paying their bills. It provides the interface needed to telecommunicate these data directly to the Authorization Center computers.

- **Smart Card Production Management** - The Subscriber Management System data is used to generate orders for the production of new subscriber viewing cards. This includes both personal data to be printed on the card and entitlement and security-related data to be programmed into the card's computer chip.

6.2 Over-the Air Addressing

The Subscriber Management System can initiate a number of actions directed at individual subscriber smart cards. It does so by sending relevant data in the specified format to the Authorization Center. The Authorization Center computers process and combine the data with the scrambled video signal for over-the-air broadcast.

Despite the fact that, with VideoCrypt™, there is no need for over-the-air cipher management, the system can address individual subscribers at a rate of between 160,000 and 3.3 million per hour.

The types of actions initiated by the Subscriber Management System are:

- **Granting an entitlement (or whitelisting)** - An entitlement (or, following blacklisting, "whitelisting") action enables viewing for a single channel or for the entire card (i.e., all channels). Following a blacklisting action against the entire card, only a similar whitelisting action (i.e., on the entire card) can be executed.

- **Revoking an entitlement (or blacklisting)** - A blacklisting action disables viewing for a single channel or for the entire card. Only a parallel whitelisting action can restore the disabled service(s). Up to seven blacklisting/whitelisting couples can be performed on a single smart card.

- **Displaying a smart card message** - This action causes a message that is pre-programmed on the smart card to be displayed on the television screen of the addressed subscriber. Messages of this type include:

  PLEASE CALL *nnnnnnn*
  PLEASE PAY YOUR BILL

  The Subscriber Management System is also capable of generating free-format messages for systemwide broadcast.

Each action is added to a database at the Authorization Center and is broadcast periodically until it expires or is deleted. To simplify card management toward the end of a smart card period, actions can be entered twice—to enable the addressing of both the current and replacement card (*see Figure 3*).

The Subscriber Management System may designate certain actions as high-priority; i.e., for immediate broadcast. In that case, a viewer can receive immediate on-screen indication that an action has been executed. As a result, the customer service operator at the Subscriber Management Center can, for example, in a single telephone call: receive an order for expanded service, generate an immediate over-the-air entitlement, and receive confirmation from the customer that the entitlement has been received.

6.3 Smart Card Production Management

Periodic replacement of smart cards is a central feature of VideoCrypt™ security. A new card is issued to every subscriber at the beginning of each new period (about every three months). Between periodic replacements, cards are issued as necessary; e.g., to new subscribers or to subscribers who report lost, stolen, or inoperable cards. Cards are generally issued inactive ("locked"), and remain so until *chained* by the subscriber to one of his/her previous cards.

Smart cards offer tremendous management flexibility. Among the elements that can be customized for each service provider are:

- security algoritms
- data transmission format
- level of smart card sophistication
- prices and methods of payment (including for pay-per-view)

Perhaps even more significant is that any of these elements can be changed at the time of the next systemwide replacement of subscriber smart cards.

Each service provider specifies the types of cards to be distributed to its subscribers. Among the options are:

- **Viewing Card** - for enabling normal viewing of the programs to which the subscriber is entitled

- **Key Card** - for overriding parental control restrictions that may be contained in the Viewing Card

- **Token Card** - for enabling the purchase of pay-per-view services by the subscriber *on impulse* (i.e., by pushing a button on the decoder). A similar type of debit card could be applied to the over-the-air purchase of a wide range of merchandise.

- **Event Card** - for enabling viewing of individual promotional programs

Among other card-distribution details set by the service provider are: situations in which to issue a new card to a subscriber, the method for delivering a subscriber's first active viewing card, and the means of distributing cards (e.g., mail, retail outlets, agents). The many options for card distribution can enable the service provider to reduce its pool of telephone operators and eliminate payment of sales commissions to third-party agents.

Regardless of the system's particular card-management parameters, issuance of smart cards is initiated at the Subscriber Management System. The Subscriber Management System sends all necessary card *personalization* information to the card production facility according to the specified data exchange format. The information (all of which is contained in the subscriber database) includes: card ID number, chaining number, expiration date, parental rating limit, entitlements, and the subscriber name and address.

Generally, systemwide replacement of cards is initiated about six weeks prior to the new period, at which time the Subscriber Management System sends tapes containing the subscriber information to the card production facility (*see Figure 3*). A month is allotted for personalization of cards, with two weeks remaining for delivery. Management of the card changeover period is simplified by enabling subscribers to use their new (replacement) cards as soon as they receive them (i.e., by making each card operable in both the current and new periods). Old cards become inoperable on the first day of the new period.

7. Conclusion

Smart cards, as applied in the VideoCrypt™ system, offer many management advantages:

- **Security** - They are detachable, replaceable, and incorporate state-of-the-art technology.
- **Low cost, low risk** - The wide selection of cards available at a range of prices enables service providers to match their security needs and budget to the right card. Because decoders are generic, they can be produced at lower cost. Finally, smart cards eliminate the risk of having to replace decoders systemwide.
- **Business flexibility** - Each service provider can customize system behavior to suit its business needs.
- **Revenue generation** - Smart cards can be used to create revenue, through merchandising, advertising, and one-time promotional events.
- **Open technology** - A system based on smart cards is protected from obsolescence because of its use of standard components and nearly endless ability to incorporate future technologies.

These advantages constitute an effective answer to many of the most pressing problems facing the pay-TV industry.

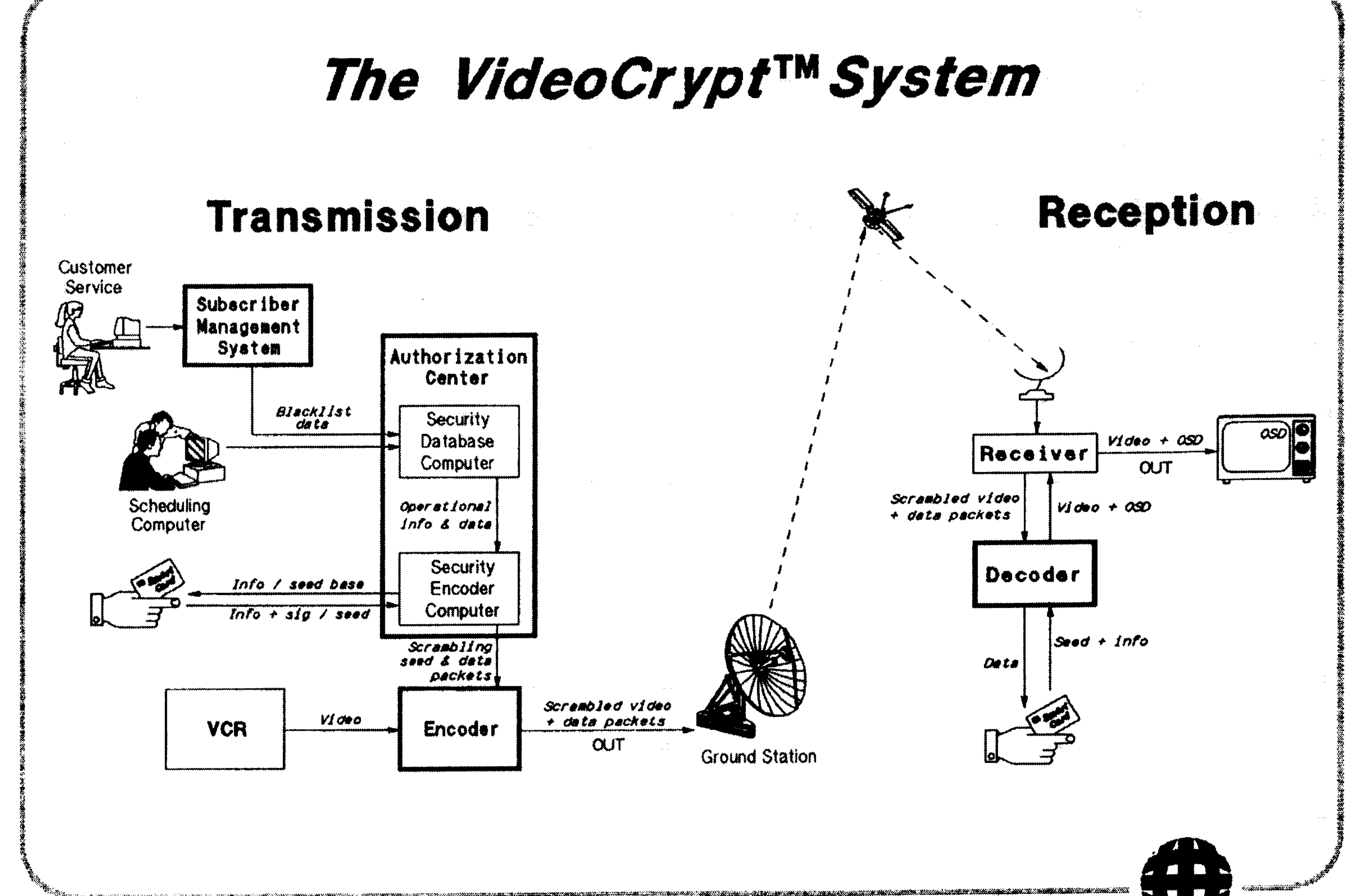

The VideoCrypt™ System
Transmission
Reception
Customer Service
Subscriber Management System
Authorization Center
Security Database Computer
Blacklist data
Scheduling Computer
Operational info & data
Security Encoder Computer
Info / seed base
Info + sig / seed
Scrambling seed & data packets
VCR
Video
Encoder
Scrambled video + data packets
OUT
Ground Station
Receiver
Video + OSD
OUT
OSD
Scrambled video + data packets
Video + OSD
Decoder
Seed + info
Data
NEWS DATACOM

Figure 1

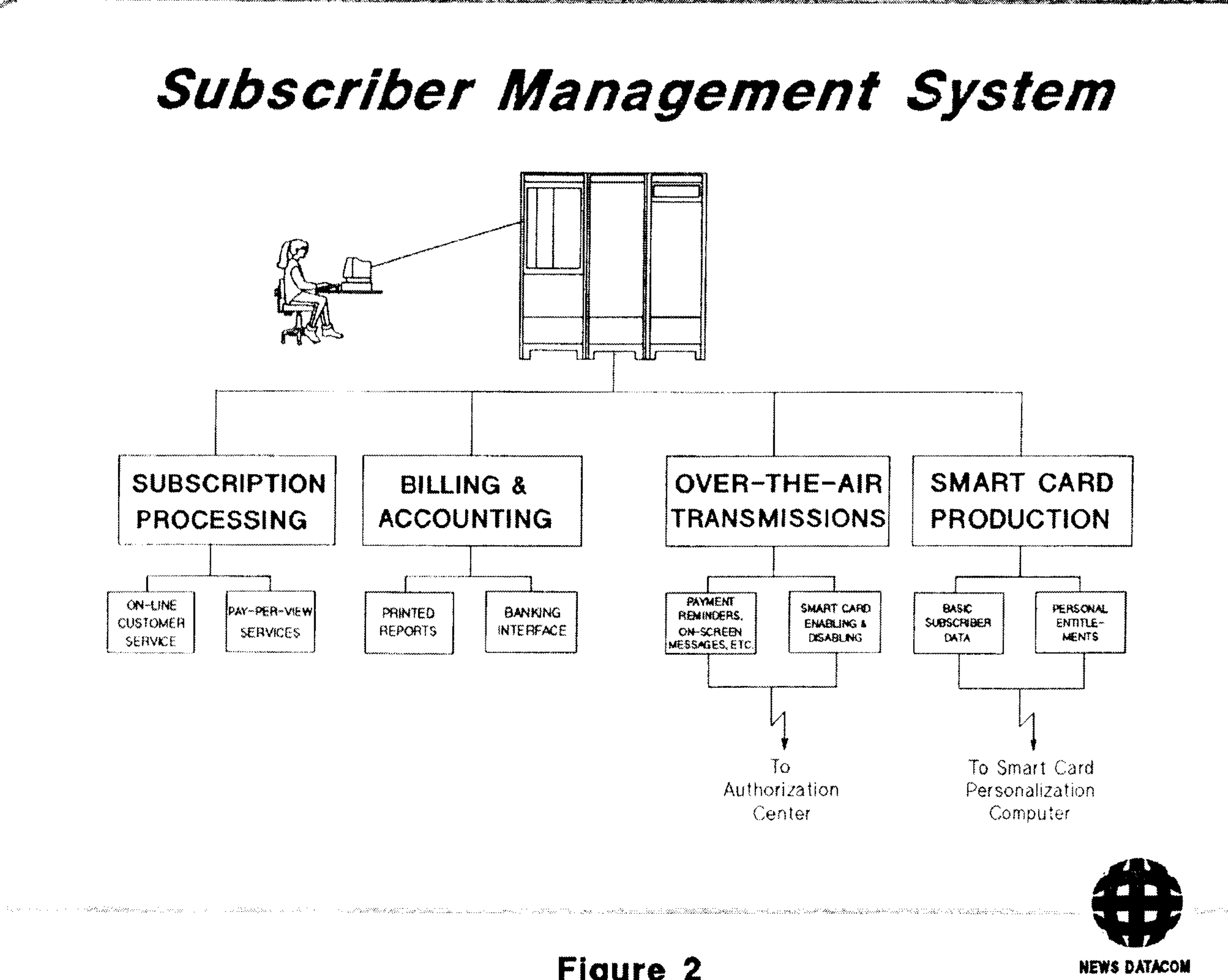
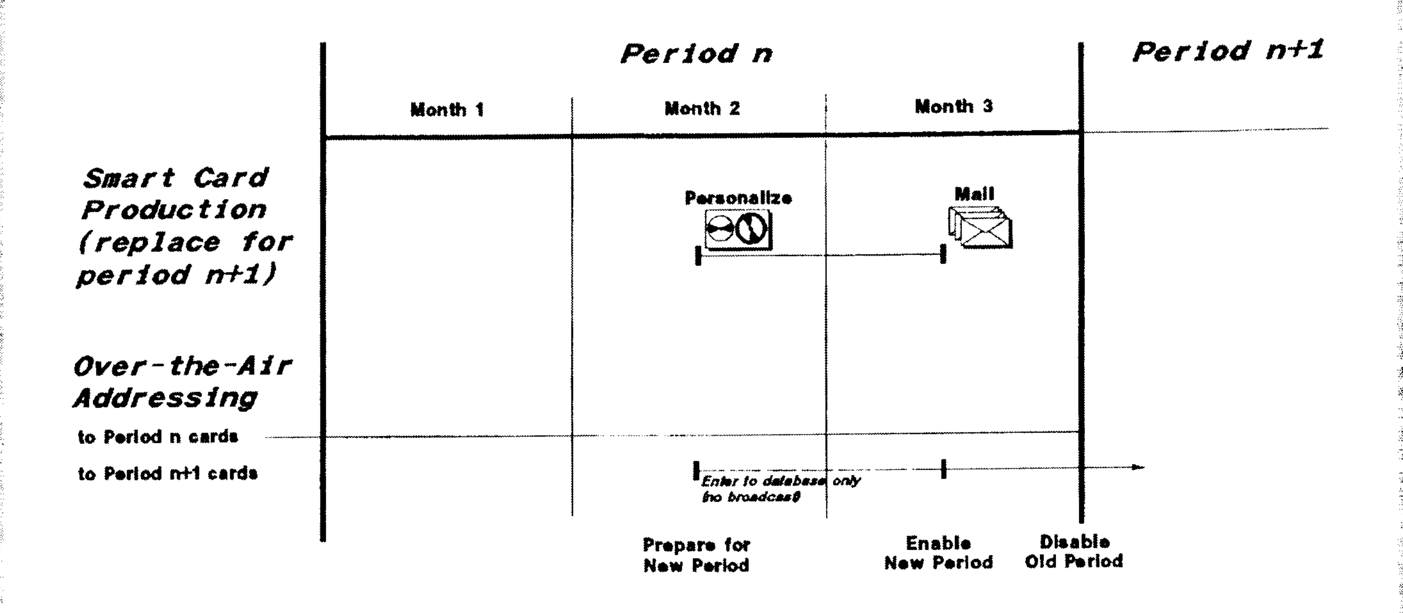

Subscriber Management System
SUBSCRIPTION PROCESSING
BILLING & ACCOUNTING
OVER-THE-AIR TRANSMISSIONS
SMART CARD PRODUCTION
ON-LINE CUSTOMER SERVICE
PAY-PER-VIEW SERVICES
PRINTED REPORTS
BANKING INTERFACE
PAYMENT REMINDERS, ON-SCREEN MESSAGES, ETC.
SMART CARD ENABLING & DISABLING
BASIC SUBSCRIBER DATA
PERSONAL ENTITLE-MENTS
To Authorization Center
To Smart Card Personalization Computer
NEWS DATACOM

Figure 2


Smart Card Management --
Quarterly Schedule
Period n
Period n+1
Month 1
Month 2
Month 3
Smart Card Production (replace for period n+1)
Personalize
Mail
Over-the-Air Addressing
to Period n cards
to Period n+1 cards
Enter to database only (no broadcast)
Prepare for New Period
Enable New Period
Disable Old Period

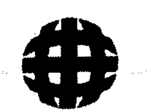

NEWS DATACOM

Figure 3

PAC MANAGER

OU LA GESTION TECHNIQUE DES TITRES D'ACCÈS CONDITIONNEL AUX SERVICES AUDIOVISUELS

Didier **CERTAIN**
SEMA GROUP
5 square René Cassin
35700 RENNES
FRANCE
Tél : +33 99 38 17 38

RÉSUMÉ

SEMA GROUP a développé un gestionnaire de titres d'accès en mode abonnement (GTA-MA) connu sous le nom de PAC Manager. Ce système trouve sa place entre les systèmes de gestion (SG) des fournisseurs de programmes et les diffuseurs de messageries (DM) des points d'émission (PE). PAC Manager assure la distribution des droits d'accès vers les abonnés en générant des messages de gestion (EMM) insérés dans le flot d'images télédiffusées. Chez l'usager, le décodeur se charge d'extraire ces messages de gestion et d'inscrire les droits d'accès dans la carte à puce associée au décodeur.

ABSTRACT

SEMA GROUP has designed and has built a subscriber's authorisation system in subscription mode (SAS-SM) which is known as PAC Manager. This system is interfaced between the subscriber's managing system (SMS) of program providers and the message broadcasters (MB) of the emission points (EP). PAC Manager has to distribute access rights toward subscribers. Access rights are distributed in the form of Entitlement Management Messages (EMM) inserted in the flow of televised pictures. At user's level the decoder extracts these management messages and writes the access rights into the smart card associated with the decoder.

TABLE DES MATIÈRES

1 - LE CONTEXTE GENERAL

1.1 - COCOONING ET HEDONISME

Pour le consommateur qui souhaite regarder le film, le match ou le concert de son choix douillettement installé chez lui devant son téléviseur, l'aventure commence chez le spécialiste hifi-vidéo en bas au coin de la rue.

C'est là en effet que notre amateur de cinéma, de sport ou de musique obtiendra le décodeur magique et la carte à puce personnelle contenant ses propres tickets d'accès.

Ainsi, à peine notre consommateur a-t-il installé son précieux matériel sous sa télé qu'il peut bénéficier de la palette d'émissions auxquelles il a souscrit. Et si par hasard il a oublié de demander tel ou tel accès privilégié, un simple coup de téléphone ou de minitel lui permettra de commander la télé-inscription par la voie des airs du ticket manquant dans sa carte.

Magie de la technique, assurément. Mais le plus étonnant dans cette innovation, c'est que grâce à la carte à puce, notre téléspectateur a pu n'acheter que les émissions et les programmes qui le passionnement vraiment.

Une télé à la carte en quelque sorte.

Rien ne lui interdit, en effet, de se payer une tranche de film, un round de match de boxe ou de choisir au coup par coup en zappant. Cependant, la profusion des programmes télévisuels et l'inélasticité du porte-monnaie du consommateur trouvent rapidement leur limite dans la télévision à abonnement classique. C'est pourquoi la télévision-passion de demain passe nécessairement par une télé à la carte.

Mais avant d'arriver à mettre en place un système complet à l'échelle européenne de télévision à la carte, il a fallu définir une politique industrielle commune pour laquelle se sont engagés les plus grands groupes industriels.

1.2 - LES NOUVEAUX PAYSAGES AUDIO-VISUELS

La dernière décennie a vu se bousculer son lot d'innovations, de débordements, de normalisations et d'imagination. La France a mis en place un ensemble d'éléments politiques, techniques et économiques connu sous le vocable de nouveau paysage audio-visuel français (PAF). Plus généralement, les pays européens ont également contribué à faire éclore un nouveau paysage audio-visuel européen (PAE).

Ces nouveaux paysages se caractérisent par un débordement hors des monopoles d'état, hors des frontières des pays et hors des normes technologiques usuelles. En effet, l'avénement des chaînes commerciales (en clair ou à péage) cohabitant avec les anciennes chaînes publiques a affaibli la notion même de monopole. D'un autre côté, l'irruption des réseaux locaux de vidéocommunication et des satellites de télévision directe (TDF1, TVSAT, ASTRA, pour ne citer que les premiers) a fait éclater les traditionnelles frontières au sol. Enfin, l'émergence d'une télévision hifi demandée par les consommateurs a nécessité de sortir des normes technologiques habituelles (PAL, SECAM) et d'entrer dans le XXIème siècle avec de nouvelles normes (D2-MAC, HD-MAC) orientées vers la télévision à haute définition.

C'est dans ce contexte résolument novateur que se place VISIOPASS, ambitieux projet voulu par FRANCE TELECOM.

VISIOPASS est destiné, à l'échelle européenne, à satisfaire les besoins de toutes les applications de télévision à péage grand public ou aux besoins de transmissions sécurisées entre professionnels, par câble ou par satellite. Le projet VISIOPASS financé et animé par FRANCE TELECOM rassemble la volonté et les moyens des plus grands groupes industriels européens (BULL, FRANCE TELECOM, MATRA, PHILIPS, SEMA GROUP pour n'en citer que quelques uns).

1.3 - LA NOUVELLE EQUATION ECONOMIQUE

Bien entendu, toutes ces innovations ont un coût et il est permis de se demander si le consommateur habitué à regarder une télé commerciale financée par la publicité est prêt à payer pour regarder une télé à la carte financée par abonnement ou par paiement à la séance.

La question est posée et les premiers éléments de réponse sont positifs. Tout d'abord, "le" téléspectateur n'existe pas : il faut segmenter les téléspectateurs en fonction de leur pouvoir d'achat et de leurs pôles d'intérêt. Ensuite, il est remarquable que le segment qui offre la meilleure solvabilité est également celui qui demande une télévision différente (plus thématique, moins "grand public", moins envahie par les écrans publicitaires). A cet égard, le succès de Canal+ mérite d'être médité. Enfin, on peut noter ça et là l'émergence d'un usage personnalisé et interactif de la télévision : pouvoir composer "à la carte" son propre programme tout en ne payant que les thèmes effectivement choisis ou les séances réellement regardées.

Pour parvenir à équiliber cette nouvelle équation économique, la télévision à péage classique est dépassée. En effet, il n'est pas envisageable d'avoir autant de décodeurs que de chaînes payantes. Que ce soit en termes d'encombrement chez le consommateur ou en termes de coût, il est de l'intérêt de tous de disposer d'un décodeur banalisé unique et de particulariser les droits du téléspectateur dans une carte à puce.

Ainsi, indépendamment des problèmes industriels de développement de bout en bout du réseau de diffusion des télévisions à péage, l'un des aspects cruciaux du projet VISIOPASS réside dans la gestion des titres d'accès des consommateurs par le biais des cartes à puce. C'est cet aspect particulier qui est traité par le gestionnaire PAC Manager conçu et développé par SEMA GROUP.

2 - LA PLACE DE PAC MANAGER DANS LE SYSTEME VISIOPASS

2.1 - D2-MAC, EUROCRYPT ET VISIOPASS

La norme européenne D2-MAC est un standard de télévision améliorée qui constitue la voie d'accès vers la télévision à haute définition.

Sans entrer dans des considérations techniques, le D2-MAC se caractérise pour le téléspectateur par une suppression des bavures, effets de moirage ou de cross color habituels avec les normes classiques en raison de problèmes d'intermodulation. Le D2-MAC apporte également un enrichissement de la transmission sonore (4 voies stéréo avec son numérique). Enfin, le D2-MAC permet d'acheminer également des données (journaux télétexte, titres d'accès télédiffusés, ...).

Eurocrypt est un système d'accès conditionnel aux services audiovisuels basé sur les principes suivants : indépendance par rapport au réseau, sécurité basée à la fois sur une clé secrète et sur un titre d'accès temporaire, et, enfin, possibilité de cohabitation dans la carte à puce de plusieurs fournisseurs de programme.

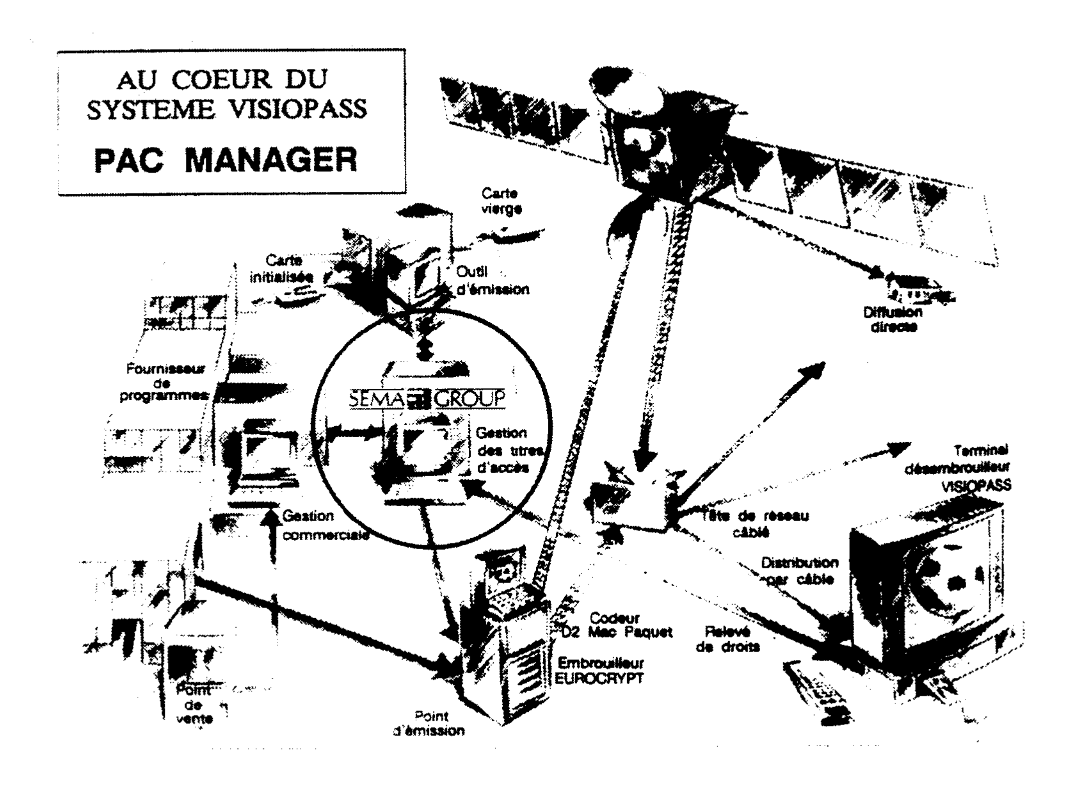
L'indépendance par rapport au réseau permet d'utiliser Eurocrypt en association avec D2 MAC aussi bien au travers de réseaux câblés de vidéocommunication que via un satellite de télévision directe.

Pour ce qui est de la sécurité, le téléspectateur doit, pour accéder au programme de son choix, disposer à la fois d'une clé secrète idoine et des titres d'accès ad hoc. Dans la pratique, la carte à puce contient en permanence la clé secrète tandis que les titres d'accès sont acheminés par voie hertzienne sur demande du consommateur. La gestion et la télé-inscription de ces titres d'accès font partie des tâches de PAC Manager.

Enfin, la cohabitation possible de plusieurs diffuseurs de programmes payants sur une même carte ouvre la voie à une authentique télévision à la carte. Le téléspectateur pourra ainsi disposer d'abonnements thématiques de séances pré-payées ou d'un crédit d'heure à consommer, ... sans se soucier de la complexité technique de l'édifice et sans exagéremment vider sa tirelire.

La norme D2 MAC et le procédé Eurocrypt permettent aux fournisseurs de programmes et aux différents acteurs du marché télévisuels (cablo-opérateurs, ...) de réaliser toutes les applications envisageables de télévision à péage. Le projet VISIOPASS est quant à lui un exemple concret et complet de mise en oeuvre de bout en bout des nouvelles possibilités offertes par la télévision à la carte.

Le schéma suivant illustre la mise en oeuvre du système VISIOPASS et la place qu'occupe PAC Manager au centre du dispositif.



2.2 - LE ROLE DE PAC MANAGER

Comme on la vu, un des points cruciaux du système VISIOPASS est la gestion des titres d'accès. Un titre d'accès est en quelque sorte un ticket d'accès, un droit d'usage, un privilège individuel qui représente la valeur achetéé par le téléspectateur. Ce ticket est inscrit dans sa carte à puce personnelle et l'autorise où qu'il soit, à voir les émissions auxquelles il a droit.

PAC Manager est la machine chargée de gérer les titres d'accès (d'où le nom de GTA). Son rôle est constitué de multiples missions :

- il gère les demandes de personnalisation de nouvelles cartes à puce,

- il gère les requêtes d'abonnement et de réabonnement qui lui sont transmises par les systèmes de gestion commerciale,

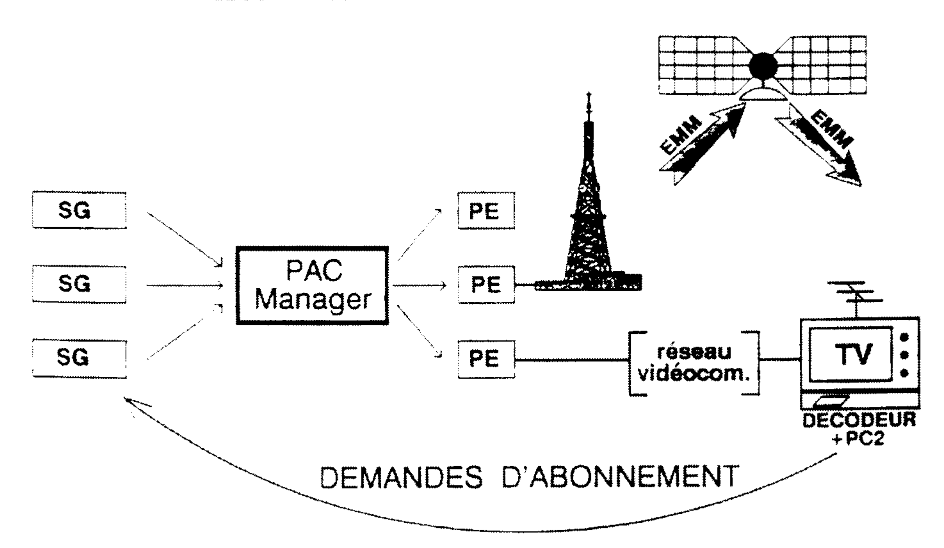
- il filtre et classe les demandes puis les regroupe avant de fabriquer les titres d'accès et d'en ordonner la télédiffusion vers les usagers.

La distribution des droits d'accès s'effectue via le diffuseur de messagerie des points d'émission. Les titres d'accès élaborés par PAC Manager sont insérés dans le flot d'images télédiffusées et acheminés jusque chez le téléspectateur.

Chez l'usager, le décodeur se charge d'extraire ces messages de gestion (appelés EMM) et d'inscrire les titres d'accès dans la carte à puce de celui-ci.

Le schéma suivant illustre ce mécanisme.

ILLUSTRATION DU MECANISME GENERAL



Un dernier point doit être noté en ce qui concerne le rôle de PAC Manager : la gestion des titres d'accès est effectuée par le système sans aucune connaissance des fichiers commerciaux des fournisseurs de programmes. Il s'agit d'une gestion purement technique de la télédiffusion des droits et donc les critères commerciaux ne sont pas et n'ont pas à être connus de PAC Manager. Ce dernier point garantit aux systèmes de gestion une totale étanchéité entre leurs fichiers de clientèle.

3 - LE SERVICE OFFERT AUX USAGERS

3.1 - ABONNEMENT

Dans le contexte de la télévision à péage, un abonnement est une prestation de service facturée en fonction de la durée de disponibilité du service et non en fonction de la durée effective d'utilisation du service.

Les trois types d'abonnements gérés par PAC Manager sont les suivants :

- abonnement par THEME/NIVEAU,
- abonnement par CLASSES,
- abonnement simple (cas particulier des deux précédents).

3.2 - ET DEMAIN, LE PAIEMENT A LA CONSOMMATION

Eurocrypt permet aussi le paiement par émission : c'est le "pay-per-view" des anglo-saxons. Dans ce cas, le consommateur n'a accès qu'au contenu de l'émission particulière qu'il a sélectionnée. Ceci peut se faire par achat anticipé, en faisant connaître à l'avance son choix au fournisseur de programme qui téléchargera le droit acheté avant l'émission ; ou bien par achat "impulsif", par action du téléspectateur sur son terminal sans avoir à prévenir a priori le fournisseur de programme. Dans ce cas, la consommation peut être organisée en mode pré-payé ou par facturation a posteriori des émissions consommées. Ce mode suppose que les informations inscrites sur la carte à mémoire sont relevées par PAC Manager. Le mode normal de télévision à péage par émission devrait être le mode d'achat impulsif avec facturation après consommation.

Eurocrypt permet enfin la taxation des émissions à la durée : c'est le "pay-per-time" des anglo-saxons. Dans ce cas, l'achat sera toujours impulsif, et le mode de facturation pourra être le pré-paiement ou la facturation après consommation.

Tous les messages techniques sont diffusés au téléspectateur en même temps que le signal vidéo, le plus souvent sous forme brouillée et sont traités automatiquement par le décodeur et la carte à puce sans intervention manuelle du téléspectateur.

3.3 - LES DIFFUSIONS SELECTIVES

PAC Manager peut envoyer des informations individuellement à telle ou telle carte à puce d'un téléspectateur. En effet, Eurocrypt permet d'envoyer aux abonnés des messages personnalisés en télétexte. Cette capacité technique peut être utilisée par les fournisseurs de programme pour un contact actif avec leurs clients.

Enfin, chacune des émissions diffusées en D2-MAC/Eurocrypt porte un code à 8 niveaux, qui est affecté à l'émission en fonction de son contenu ou de son coût. L'abonné au programme (les parents en général) peut décider de rendre obligatoire l'emploi d'un code secret (le code parental) lorsque le niveau dépasse une valeur prédéterminée. Il est prévu en cas d'oubli du code parental de télécommander la remise à zéro de ce code secret dans une carte donnée.

4 - LES PRESTATIONS FOURNIES AUX SYSTEMES DE GESTION COMMERCIALE

4.1 - LES REQUETES DE GESTION

Une requête de gestion émanant du système de gestion commerciale d'un opérateur constitue un tout indivisible et est véhiculée sous forme d'un fichier.

La structure générale d'un fichier de requête de gestion est la suivante :

- préfixe,
- protocole,
- nom du fichier,
- sceau d'authentification,
- horodate de la requête,
- longueur de la requête,
- contenu de la requête.

Le préfixe est un détrompeur qui permet de connaître le fichier. Le protocole précise le type de syntaxe et de sémantique à mettre en oeuvre pour interpréter la suite du fichier. Le nom du fichier est le nom externe sous lequel la requête de gestion est connue du système informatique. Le sceau d'authentification est le résultat du calcul d'authentification portant sur l'identité du SG, sur l'horodate de la requête et sur le contenu exhaustif de la requête de gestion.

Le contenu d'une requête de gestion est constitué de deux sous-ensembles d'informations : les modalités de diffusion et le contenu à diffuser.

Les modalités de diffusion contiennent les paramètres suivants :

- identificateur du fournisseur de programme (PPID),
- référence de diffusion (RDIF),
- conditions supplémentaires (CSUP).

Le couple (PPID, RDIF) constitue solidairement un critère de sélection des modalités de diffusion (par canaux et par période calendaire) qui sont stockées dans le fichier des références de diffusion de PAC Manager.

Les conditions supplémentaires CSUP représentent des informations dont la signification n'intéresse que le SG demandeur et le PE destinataire. Ce champ CSUP n'est pas interprété par PAC Manager ; il est transmis tel quel vers le diffuseur de messagerie du PE.

Le contenu à diffuser se présente sous la forme d'une liste de titres, de droits et de destinataires. Selon la nature de la requête (titres d'accès, droits gratuits, RAZ de PIN, invalidation), la présentation de la liste diffère quelque peu. La nature de la requête est précisée dans un préfixe de liste indiquant le type d'EMM (G0, S0, U0, U1, U2). A la suite du préfixe, se trouve la liste proprement dite. La structure de la liste dépend du type G, S ou U et du sous-type 0, 1 ou 2.

4.1.1 - Abonnement

Il s'agit de diffuser des messages de type EMM-S0 ou EMM-U2 qui véhiculent des titres d'accès (abonnement entre telle et telle date pour tel thème et tel niveau ou pour telles classes). Les EMM-S0 correspondent à des envois collectifs pour des usagers partageant une adresse commune tandis que les EMM-U2 correspondent à des envois sélectifs pour un destinataire unique.

4.1.2 - RAZ de code porteur

Il s'agit de diffuser un message de type EMM-U0 véhiculant une instruction qui remet à zéro le code parental de la carte à puce visée. Les EMM-U0 correspondent à des envois sélectifs pour un destinataire unique.

4.1.3 - Invalidation

Il s'agit de diffuser un message de type EMM-U1 destiné à invalider un service dans une carte ou même une carte complète. Les EMM-U1 correspondent à des envois sélectifs pour un destinataire unique.

4.1.4 - Diffusion générale

Il s'agit de diffuser un message de type EMM-G0 véhiculant un titre gratuit d'abonnement. Les EMM-G0 correspondent à un envoi général sans aucun filtrage d'adresse. Tout usager peut recevoir le titre gratuit sans aucune exclusion.

4.2 - LES REQUETES D'EMISSSION

Pour mettre en oeuvre la distribution des droits d'accès par voie hertzienne sous forme d'EMM télédiffusés en même temps que le signal vidéo, il faut les cartes à puce installées dans les décodeurs grand public soient pré-formattées de manière "ad hoc". Cette opération de pré-formatage que l'on appelle "émission" et qui consiste à inscrire dans la puce un certain nombre d'indications idoines est un préalable nécessaire à l'usage de la carte par le grand public. Pour effectuer l'émission des millions de cartes à puces PC2 concernées à terme par l'opération, il faut un outil d'émission itérative (OE) spécialisé à cet effet.

Outre les cartes d'abonné, l'OE permet également d'émettre d'autres catégories de cartes PC2 en petite quantité (cartes mères, cartes d'authentification). L'outil d'émission utilise, comme matière première, des cartes vierges livrées par un fabricant après encartage. Sur l'ordre de PAC Manager qui fournit des indications d'émission sous forme de scénario, l'OE initialise les cartes vierges en y ouvrant une zone "émetteur" et des zones "service". A l'issue de l'émission d'un lot de cartes PC2, l'OE communique à PAC Manager un compte rendu d'émission.

5 - LA CONFIGURATION TECHNIQUE

- Système informatique UNIX avec une configuration standard (les premières implémentations utilisent le système d'exploitation 386/IX) :

  . mémoire RAM,
  . disque magnétique,
  . lecteur-enregistreur de disquette MS-DOS 5.25",
  . streamer,
  . ports série,
  . accès X25,
  . terminaux clavier-écran.

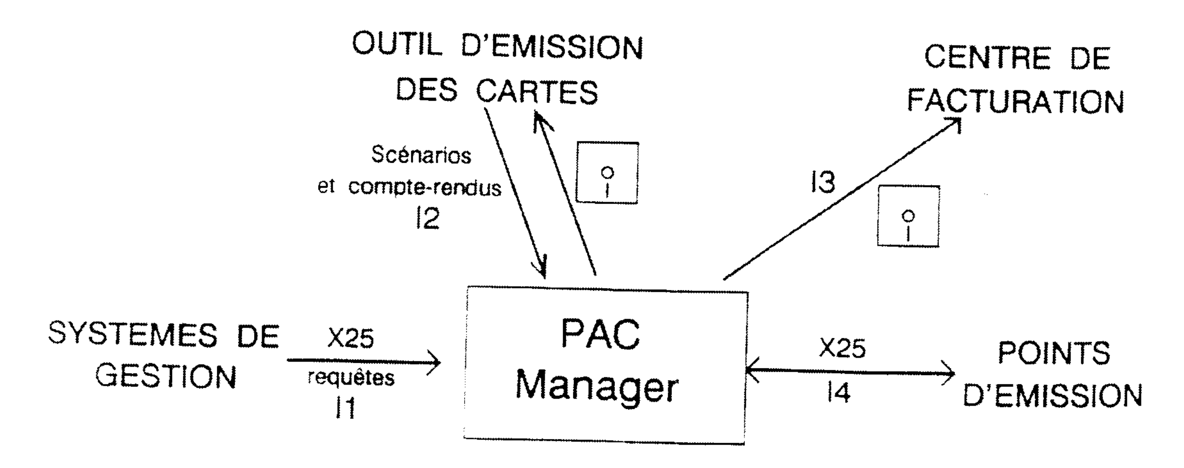
- Système de gestion de base de données relationnelle UNIFY.

- Sous-système de calcul (SSC) :

  . micro-ordinateur MS-DOS avec un accès X25,
  . lecteur de carte à mémoire BULL TLP 224.

Sur le double plan qualitatif et quantitatif, ces configurations exactes sont déterminées en fonction de l'environnement d'installation et des exigences fonctionnelles et de performances.

Les différents éléments de l'environnement fonctionnel de PAC Manager contribuent à faire circuler les données en provenance de PAC Manager ou à destination de PAC Manager selon quatre axes matérialisés par quatre interfaces (I1, I2, I3, I4).



L'interface I1 est le lien uni-directionnel entre les SG et PAC Manager. Cette interface a pour support un protocole d'échange au-dessus d'une liaison X25.

L'interface I2 est le lien bi-directionnel entre l'OE et PAC Manager. Elle permet d'échanger scénarios d'émission et comptes rendus d'émission. Cette interface a pour support une disquette MS-DOS de 5"1/4 pouces formattée à 1.2 Moctet.

L'interface I3 est le lien uni-directionnel provenant de PAC Manager à destination du centre de facturation. Cette interface a pour support une disquette MS-DOS de 5"1/4 pouces formattée à 1.2 Moctet.

L'interface I4 est le lien bi-directionnel entre PAC Manager et les PE. Cette interface a pour support un protocole d'échange PAC Manager-diffuseur de messagerie au-dessus d'une liaison X25.

6 - CONCLUSION

Actuellement, PAC Manager a été conçu pour le mode abonnement, mais il ne demande qu'à grandir et les tout prochains développements sont destinés à prendre en compte le paiement à la séance (pay-per-view) et la téléinscription de nouveaux services.

Le système a déjà fait ses preuves dans le cadre des balbutiements du projet VISIOPASS, il ne lui reste plus qu'à croître et embellir. C'est ce que nous lui souhaitons ici en France mais également dans le monde entier.



<u>C'est possible avec **PAC Manager** !</u>

THE NORWEGIAN TELECOM'S SYSTEM

FOR CUSTOMER MANAGEMENT

Jon **NORSTEBØEN**
Norwegian Telecom Administration
PO Box 83
2007 KJELLER
NORWAY
Tél : +47 6 809163

ABSTRACT

This paper gives an overview of the conditional access functionality provided by the Eurocrypt-S system.
It summarizes the customer management function which must be provided to perform access control for broadcast services based on the Eurocrypt-S system.
Norwegian Telecom has developed a complete system for customer management based on Eurocrypt-S. The first version of this system is now in operation for D-MAC/Eurocrypt-S transmissions via INTELSAT. The paper gives an overview of the current existing system and the next generation system being developed.

TABLE OF CONTENTS

1. INTRODUCTION

Norwegian Telecom (NT) has for several years been involved in Satellite Broadcasting and programme distribution using the MAC/Packet standard. The Norwegian national program, NRK and the two public channels of Sweden, have been distributed to Norwegian viewers using C-MAC since 1984 and 1986 respectively. In the process of introducing conditional access on these transmissions they are now converted to D-MAC which is now the official standard for satellite broadcasting in the Nordic countries.

NT has been one of the leading bodies in the standardization of conditional access system for the MAC/Packet standard. This work has lead to the NR-MSK/EUROCRYPT-S specification which fulfils the known requirements for efficient conditional access using MAC. The specification is now adopted by the NR-MSK/Nordic countries.

NT has established an organization for customer management which will offer customer and equipment management services to all programme providers using D-MAC reaching Norwegian ground. The management services will be offered for individual reception both in cable networks and DTH.

Based on the NR-MSK/EUROCRYPT-S standard, NT has supported development of all the components which is required in a customer management system. This includes

- in cooperation with KVATRO, development of database systems for efficient customer and equipment management

- in cooperation with Tandberg Telecom, KVATRO and Broadcast Systems Software, development of channel controllers for efficient interfacing to MAC/Packet multiplexing equipment

- in cooperation with Tandberg, development of MAC receivers based on the Nordic/Phillips/Plessey design of chip sets

- in cooperation with Nordic VLSI, development of CASS software, starting with a prototype based on a professional high cost component and now using highly secure and low cost smart card processors

The NT customer management system is installed at Nittedal earth station near Oslo and has been operating since October -89. The system is now used for management of the Swedish programmes to Norwegian viewers, but will later be made available to several programme providers. The customer management system will make several programmes and channels to be received using the same decoder. The system is cost beneficial being a shared resource between a number of TV channels. The system is able to support programmes being multiplexed and uplinked also outside Norway.

This paper outlines the requirements for a conditional access system for broadcast services in terms of

- the technical elements involved
- the functions which must be provided
- the organizational structure which is required
- the equipment which is needed to perform the customer management

The paper outlines how the technical and functional requirements are met in the NR-MSK/EUROCRYPT-S specification and by using this specification; how the NT development meets the requirements for a flexible customer management structure performing sales of broadcast services to a large amount of customers.

2. SUMMARY OF EUROCRYPT-S CONDITIONAL ACCESS SYSTEM

2.1 TECHNICAL ELEMENTS

A conditional access system for broadcast services is based on the five basic elements:

1. The scrambling function
2. The encryption and decryption algorithm(s) and key(s)
3. The secure storage device
4. The addressability of the receiver population
5. The upgradability of the functions of the system

The SCRAMBLING FUNCTION is the physical process which is applied to the source signals, i.e. the video and the sound to make it non-interpretable. To make the transmitted signal interpretable any receiver must be equipped with a descrambler unit.

In the MAC system the scrambling function is digital. Active line rotation is applied to the video and a pseudo random bit sequence is applied to the sound. The scrambling function is made time variant by using a Control Word which can be changed every ten seconds.

The ENCRYPTION algorithm is a set of mathematical operations which "spreads" the information of a message in a way that it is not interpretable. A receiver must have the appropriate decryption key and algorithm to get the message in clear.

To ensure that none of the algorithms, the encryption keys and the entitlements protecting the services are compromised, this information must be processed and stored in a SECURE DEVICE. This is the CASS (Conditional Access Sub System) of a receiver. The CASS performs like a black box. It receives encrypted messages containing keys and entitlements. The CASS returns the right control word for descrambling of the service if the right keys and entitlements are contained in the CASS.

To ensure that each individual receives the correct entitlements, the CASS population must be ADDRESSABLE. To ensure this each CASS has it's own unique identity and a corresponding unique decryption key. If the programme channel has spare digital capacity, messages to each CASS can be transmitted in the channel. This is over air addressing. To make the message transport more efficient, a set of group addresses are defined. Individuals having common entitlements are members of the same groups.

To ensure UPGRADABILITY the CASS functions are separated from the MAC decoding functions. New functions and higher security can be obtained as the capacity of the CASS components increases. Having a detachable CASS component ensures that entitlements can also be distributed to the customer without using over air addressing if this is not applicable.

2.2 CONDITIONAL ACCESS FUNCTIONS

This section gives a summary of the conditional access functions provided in the Eurocrypt-S system.

2.2.1 FUNCTIONS RELATED TO SALES

A conditional access system for broadcast services must support the three basic sales methods:

I. SUBSCRIPTION to a service or a subset of the service.
II. PREBOOKING of special programmes or events
III. IMPULSE PAY PER VIEW

NR-MSK/EUROCRYPT-S supports all these functions.

The first method: SUBSCRIPTION allows the customer to order a set of services for a certain time period. Subscription services are mostly prepaid. At the end of a period a customer can continue with the same subscription packet or he can change it.

NR-MSK/EUROCRYPT-S offers several subscription modes.

Static subscription mode is suited when the services are offered to the customer for a long period.

When operating a service in dynamic subscription the customer is allowed to change his subscription frequently. Dynamic subscription mode has in addition many features to make very specific or "tailored" subscription packets available to the customer. Examples are subscription to specific programme types or themes, to specific time slots during the day and to specific service components.

The second method: PREBOOKING is used for sale of specific programme, programme series or special events. Prebooking may be pre- or postpaid. To make prebooking for sale of programmes efficient, a well developed marketing system is required.

The third method: IMPULSE PAY PER VIEW allows the customer to buy a set of money tokens to be used for one service or a set of services. The tokens are consumed as the customer watches the programmes. The tokens may be decremented for each time unit or for each programme.

To achieve viewing statistics when operating in impulse pay per view mode, some return channel must be available either in the programme channel, via the telecom network or by use of smart card terminals connected to the management system.

2.2.2 FUNCTIONS USING GEOGRAPHICAL AND LOGICAL ADDRESSING

In addition to the sales method the conditional access system must also support functions which transmits messages to the customer via the channel and efficient methods to adapt the programme to national legislation. In NR-MSK/EUROCRYPT-S this is implemented by using teletext assisted by geographical/logical addressing.

Functions using geographical or logical addressing are

I. REPLACEMENT
II. PAGE
III. FINGERPRINT

Most of these functions are used in interaction with a teletext service.

The REPLACEMENT function is used to adapt the programme to national or regional legislation or to restrict the reception of a certain programme to the area in which the copyrights applies. Video is replaced with a locally or remotely generated teletext page. The original sound is replaced with another sound channel of specified language.

The PAGE function is used to send messages via teletext to individuals or customer groups. The page function is suited for direct marketing or to distribute any other information to a customer or group of customers.

The FINGERPRINT function is used to prevent and optionally detect pirate reception and copying of programmes. By a command sent along with the programme all or a specified groups of receivers are enforced to print their unique serial number on the screen during a short time interval. Any pirate copy of a programme will contain this fingerprint and can easily be traced to the source of it.

2.2.3 FUNCTIONS RESTRICTING THE ACCESS TO THE CASS/DECODER

To restrict the access to the decoder, Eurocrypt-S offers a mechanism for user authentication.This is obtained by a secret code (PIN code) exchanged in a user dialogue between the user and the CASS.

This user authentication is useful to

- make theft of the detachable CASSes (smart cards) less attractive.

- to restrict the use of the CASS to the owner or people the owner authorize

3. CUSTOMER MANAGEMENT SERVICE FOR BROADCAST SERVICES BASED EUROCRYPT-S

NR-MSK/EUROCRYPT-S offers a set of functions to provide conditional access for broadcast services using the MAC standard. A customer management organization can apply these functions to make the services and programmes available to a large population of customers. To do this, the customer management must somehow complete the following tasks:

3.1 SUMMARY OF CUSTOMER MANAGEMENT TASKS

I. CASS logistic:
Make the CASS components with the appropriate interfaces, functionality, security and unique addresses and keys available to the customer.

II. Programme "logistic" or marketing:
Make the services and programmes known to the customer in a way that he wants to buy them. The services and programmes may be marketed using a variety of sales methods, prices and special offers adapting to regional or national interests, habits and legislation.

III. Entitlement flow:
The transport of encryption keys and entitlements which ensures that compatible entitlements and keys are contained in the security modules both at the transmitting and the receiving side. In other words: The CASS content must reflect the entitlement coding of each programme. The marketing and sales methods will have large effect on the entitlement flow.

IV. Money flow:
To ensure that the customer pays at the right time and that the money is shared among the parties involved: copyright owner, programme provider, signal carrier and customer management.

To complete these tasks, the customer management must have a TECHNICAL SUPPORT SYSTEM which ensures that the right modules and the right information are at the right place at the right time without too much effort and without loss of security and control.

In addition the customer management must have the ORGANIZATION AND THE INFRASTRUCTURE to serve both the customer and the programme provider satisfactory.

NT has developed the technical system which today is used for a D-MAC/EUROCRYPT-S operational service. This system is now being further developed to allow a decentralized organization to handle a large amount of individual customers.

NT has also established an organization which in parallel with the technical development shall build up the infrastructure which is required to handle a lot of individual customers. The next sections give more details of the organizational infrastructure and the technical support system which is being developed by the NT.

3.2 CUSTOMER MANAGEMENT ORGANIZATION AND INFRASTRUCTURE

The customer management organization has central and decentral functions. The organization must handle both market related subjects and advanced technical systems. The organization may be divided into 4 parties: the CASS issuer, the Customer Management Centre, the Local Agents and the Service Control Centre.

3.2.1 CASS ISSUER

The CASS issuer performs the CASS loading and distribution.

The CASS is the security module of the receiver. A basic CASS contains

- Software which provides the Eurocrypt functionality, the decryption algorithms and the interface protocol to the receiver.

- Storage capacity for decryption keys, customer addresses and entitlements for several channels.

Before the CASS can be used by a customer, some additional information must be loaded into the CASS. The CASS issuer performs this:

- makes the CASS secure and addressable by loading a unique serial number and a corresponding unique key.

- makes the CASS suited for a country or a programme channel by adding extra functionality and single or multi language capability for user dialogue

- distributes the CASS modules to the right party along with the unique keys to make the party able to load his specific keys and entitlement into the CASS.

3.2.2 SERVICE CONTROL CENTRE

The service control centre is responsible for the "entitlement flow" in the system. The service control centre performs a technical function ensuring that compatible entitlements and keys are contained in the security modules both at the transmitting and the receiving side. In other words: The CASS content must reflect the entitlement coding of each programme.

The marketing and sales methods will have large effect on the entitlement flow in the system. The degree of decentralization of the management structure will also have effect on the entitlement flow. As an example: If the local agent perform the authorization of each CASS at his local site, he needs to have all the programme and service entitlements available on his system. If all the encryption is performed in a central system, the local agent only needs access to the commercial information i.e. the customer and programme information.

3.2.3 CUSTOMER MANAGEMENT CENTRE

The customer management centre is responsible for one population of CASS modules. This responsibility includes programme logistic, marketing and money flow and entitlement flow in the management structure for one CASS population.

The customer management centre cooperates with the programme provider on marketing of the programmes.

The customer management cooperates with the service control centre to make the entitlement flow efficient.

To make the services and programmes available to the customer, the management centre has a network of local agents in the regions he has the right to sell the programmes.

The management centre is also responsible for the money flow from the management structure to the programme provider. The income from the customers is shared among the parties involved: copyright owner, programme provider, signal carrier, central and local customer management.

3.2.4 LOCAL AGENTS

The programmes are marketed and the customers are authorized using a network of local agents. The local agent site is the point of sale in the system. The local agent may belong within the same organization as the central management or he may be independent. An independent local agent may be cooperating with several management centres.

The local agent perform authorization of customers and CASSes on the site, but also through the management centre to the uplink to address remote CASSes over air.

4. NT/EUROCRYPT-S CUSTOMER MANAGEMENT TECHNICAL SUPPORT SYSTEM

Customer management of broadcast services is a complex matter. NT has high competence and long experience with such systems.

NT is developing the technical system which is required for customer management of a large number of individual customers for several programme and service providers.

4.1 DESIGN RULES

The FUNDAMENTAL DESIGN RULES has been to build a system which

- is complete system for conditional access, including customer management systems on the transmit side and CASS/Smart Card components for the receive side.
- is easy upgradeable in functionality, security and size
- fulfils the requirements of programme providers as well as the customers
- is able to start from a small low cost centralized system and gradually increase into a decentralized system with a large number of local agents.
- is able to authorize customers for services and programmes transmitted from any uplink.

NT has development of all the components which is required in a customer management system. This includes

- in cooperation with KVATRO, development of database systems for efficient customer and equipment management
- in cooperation with Tandberg Telecom, KVATRO and Broadcast Systems Software, development of channel controllers for efficient interfacing of customer management system to MAC/Packet multiplexing equipment and studio scheduling systems
- in cooperation with Tandberg, development of MAC receivers based on the Nordic/Phillips/Plessey design of chip sets for the professional market
- in cooperation with Nordic VLSI, development of CASS software, starting with a prototype based on a professional high cost component and now using highly secure and low cost smart card processors. The smart card is compatible with the ISO-7816 standard.

4.2 DESCRIPTION OF CURRENT OPERATIONAL SYSTEM

The first version of the NT customer management system is installed at Nittedal earth station near Oslo and has been operating since october -89. The system is used for management of the Swedish national programmes which is transmitted via INTELSAT in D-MAC with [illegible] MCK/EUROCRYPT-S to Norwegian viewers

The current system has centralized all the customer management functions into one database system which perform

- CASS issuing, i.e. loading of unique keys into CASS and secure storage in database.

- Entitlement "compiler" which transfers channels, services and programmes into entitlement coding as defined in Eurocrypt-S

- on-line authorization and deauthorization of receivers in static and dynamic subscription mode. (as defined in EUROCRYPT-S). Authorization is performed by over air addressing in the D-MAC channel.

- replacement and fingerprint functions.

- billing

The system is operated by a central organization. Customer contact is via telephone.
The system is now being further developed to allow

- secure interfacing to local agents

- interfacing to remote multiplexing/uplink point

4.3 DESCRIPTION OF NEXT GENERATION SYSTEM BEING DEVELOPED

A next generation of this system will make it interface to a large number of local agents which perform the on-line authorization of the customers and CASSes. New sales functions (prebooking, impulse pay per view) is also added.

The customer management system will make several programmes and channels to be received using the same decoder. The system is cost benefit being a shared resource between a number of TV channels.

The next generation system will include

CASS ISSUER EQUIPMENT

- based on smart card technology: efficient loading of CASSes

- Based on secure storage components: distribution of CASS individual keys along with the batch of individual CASSes.

EQUIPMENT FOR SERVICE CONTROL CENTRE

- Establish structure of entitlement coding depending on marketing strategy and programme schedule of the programme channel

- Distribution of updated entitlement coding to all customer management centres and to multiplexing sites

SYSTEMS FOR CUSTOMER MANAGEMENT CENTRE

The technical system for the customer management centre is based on the current existing system. New functions is added on to allow

- Secure communication with a large number of local agents

- Secure communication with a number of remote channel controllers sited at the multiplexing point.

- New sales functions (pay per view)

LOCAL AGENT EQUIPMENT

The Local agent equipment will serve the point of sale for CASS and programme channels for the following functions

- As coordinated from the management entre in cooperation with the programme provider: marketing of available programmes

- Register Customer information, establish method of payment for a customer. The system will also be able to handle customers who want to be anonymous.

- First time authorization of CASS for one or more programme channels i.e. load the CASS with entitlements

- Report of sales and authorized CASSes to the management centre
- Collecting viewing statistics in case of services operated in impulse pay per view mode.

The local agent equipment will be cable of authorizing CASSes on the local agent site but also through the management centre to the multiplexing point for over air addressing of CASSes

CHANNEL CONTROLLER EQUIPMENT

The channel controller equipment is interfacing the on-line studio scheduling system, the service control equipment and the customer management system. The channel controller provides secure storage of entitlements and keys for encryption of service management messages as defined in Eurocrypt. The channel controller also contain a buffer for transmission of encrypted authorization messages loaded from the customer management centre.

5. CONCLUSION

Eurocrypt-S is a system which fulfils all the known requirements for conditional access for broadcast services. The full Eurocrypt-S specification is now implemented and tested and the first commercial products and systems are already available. New generation of products are being developed.

Norwegian Telecom has today a operational technical system and an organization for conditional access based on Eurocrypt-S. Norwegian Telecom has the strategy to offer these conditional access services to programme provider that want to market their programme to Norwegian viewers. The system is independent of the site of multiplexing.

Openness, flexibility and general interfaces has been the major design parameters of the NT system based on Eurocrypt-S. This makes the components in the system modular. Interfacing to MAC decoding equipment at the receive side and to studio and MAC multiplexing equipment on the transmit side is easy to achieve.

UTILISATION DES MÉTHODES

D'ACCÈS CONDITIONNEL

POUR LA DISTRIBUTION DE DONNÉES

EN NORME MAC/PAQUET

André L. **BUELENS**, W.VLEESSHOUWER
Agence Spatiale Européenne
ESTEC - PO Box 299
2200 AG NOORDWIJK
PAYS-BAS
Tél : +31 1719 84125

RÉSUMÉ

L'introduction de la diffusion de données en norme MAC/paquet nécessite la définition de nouveaux mécanismes et protocoles, basés sur l'extension des fonctions déjà existantes. L'utilisation des méthodes d'accès conditionnel présente certaines limitations pour les services transmettant de faibles quantités d'information à des destinataires continuellement changeants. Ces problèmes peuvent être résolus en combinant les méthodes d'accès conditionnel avec les possibilités d'adressage définies dans le protocole de transport des services de données, offrant ainsi toute la flexibilité requise pour les différents modes d'opération.

ABSTRACT

The introduction of data broadcasting in MAC/packet requires the definition of new mechanisms and protocols based on the extension of the existing facilities. The use of conditional access systems presents some limitations for services transmitting low volumes of data to constantly changing receivers. These problems can be solved by combining conditional access mechanisms with the addressing capabilities defined for the transport protocol. This provides data services with the required flexibility for the full range of operational scenarios.

TABLE DES MATIÈRES

UTILISATION DES METHODES D'ACCES CONDITIONNEL POUR LA DISTRIBUTION DE DONNEES EN NORMES MAC/PAQUET

A.L. Buelens

1. Introduction

La diffusion terrestre de télétext, transmis durant le retour de trame d'une image TV, est chose courante dans plusieurs pays Européens depuis plusieurs années. La capacité, relativement modeste, du télétext est fonction du nombre de lignes allouées à ce service entre chaque trame vidéo.

L'introduction des satellites de télédiffusion directe marque une nouvelle ère avec l'avènement d'un nouveau standard de transmission, le MAC/paquet. Le nouveau système, défini par l'U.E.R. et objet d'une directive de la C.E.E. en faisant le standard pour la diffusion directe par satellite en Europe, offre des images vidéo de haute qualité, accompagnées de sons numériques et de transmission de données.

Une ligne, en codage MAC, est partagée entre la transmission en séquence des signaux de luminance et chrominance, et une salve de données duobinaires contenant la partie numérique (voies sonores et services de données) du signal. La juxtaposition de ces salves de données sur une trame complète forme une sous trame appelée le multiplex paquets. La transmission des données numériques s'effectue par paquets ayant une longueur de 751 bits et différenciés au moyen d'une adresse de paquet comprise entre 0 et 1023. Une voie sonore est transmise par des paquets ayant une même adresse, allouée au service pour la durée de sa présence dans le signal.
Le télétext traditionnel, transmis durant le retour de trame, est toujours présent et remplace les signaux de luminance et chrominance sur les lignes correspondantes lorsqu'il est transmis. Les services de données, au sens général du terme, utilisent également la structure de paquet et sont transmis dans le multiplex numérique. De même que pour les voies sonores, la distinction entre différents services s'effectue au moyen de l'adresse de paquet qui reste fixe pour un service durant tout le temps de sa présence dans le signal.
Ainsi défini, le signal MAC/paquet est un multiplex de différents services dont la structure varie en fonction du temps. Pour cette raison, un système d'identification des services, transmis avec une adresse de paquet égale à zéro, informe le récepteur sur la configuration à adopter suivant les services souhaités. Le standard MAC/pacquet prévoit les différents mécanismes permettant d'effectuer un contrôle de l'accès aux différentes composantes du signal et permet de définir, de façon dynamique durant la transmission, les groupes d'utilisateurs autorisés à recevoir un service. Ce sont les méthodes d'accès conditionnel.
Finalement, un mode d'opération, dit plein canal, permet en l'absence de signal vidéo de remplir la totalité de la trame avec des paquets de données. Le débit binaire total du canal devient dans ce cas 10,125 ou 20,25 Mbps (respectivement D2 ou D MAC) à comparer aux 1,5 ou 3 Mbps (respectivement D2 ou D MAC) disponibles en mode normal.

Le travail de définition des standards MAC/paquet s'est effectué en plusieurs étapes. Une première étape vit la spécification des protocoles pour les services dit traditionnels: vidéo, voies sonores et télétext dans le retour de trame. Cela comprend les règles de codage, la définition de la voie d'identification des services (paquet 0) et les méthodes d'accès conditionnel. L'introduction des services de données nécessita une extension de la norme pour définir une structure de codage propre et l'adaptation des facilités existantes à leurs besoins spécifiques.

2. Les services de données et leurs besoins spécifiques

Le terme service de données recouvre, sans aucune restriction, tout type d'applications possibles et imaginables. En se référant au modèle de l'ISO, le protocole MAC fournit les fonctions de transport correspondant aux couches 1 à 3, les niveaux supérieurs demeurant entièrement la responsabilité du fournisseur de service. L'exemple le plus simple est le transfert d'un fichier de données. Mais le service peut aussi faire appel à un protocole d'application défini selon les couches 4 à 7 du modèle de l'ISO et adapté à la transmission unidirectionnelle, si nécessaire.

Dès lors on peut imaginer différents scénarios d'utilisation de cette fonction de transport qui peuvent être regroupés en deux catégories:

- Dans un premier scénario, le fournisseur de service transmet l'information de façon continue à une population d'utilisateurs importante et figée dans le temps.
- Le second scénario est celui dans lequel le fournisseur de service envoit un court message destiné à un groupe restreint d'utilisateurs ou même à un utilisateur unique. Dans ce second scénario, la définition de la destination change à chaque nouveau message.

Nous voyons donc que les deux paramètres qui permettent de caractériser un service de données sont la longueur, ou la taille, de l'information à transmettre et le nombre d'utilisateurs à qui l'information est destinée.

Les principes de base qui ont guidé le développement des protocoles pour la transmission des services de données sont les suivants:

- utiliser autant que faire se peut les structures déjà existantes, définies pour le MAC/paquet;
- développer un système de transmission entièrement indépendant de la nature des services et fonctionnant de façon totalement transparente;
- définir uniquement les fonctions de transport des données, et fournir suffisamment de flexibilité dans l'opération du protocole que pour autoriser différents modes de transmission en fonction des besoins propres de chaque service;
- concevoir un protocole suffisamment résistant que pour opérer en diffusion, c'est à dire par définition sans ligne de retour des utilisateurs vers le transmetteur.

Partant de ces idées de base et afin de satisfaire les différents scénarios décrits plus haut, les facilités suivantes sont requises pour le protocole de transmission:

- pouvoir détecter et/ou corriger les erreurs afin de pallier à la nature unidirectionelle de la transmission. Pour ce faire, les fonctions existantes, codage de Golay et/ou CRC sont réutilisées;
- l'embrouillage de certains services, pour des raisons de sécurité ou de redevance, suivant les méthodes existantes d'accès conditionnel;

- fournir, pour les applications faisant appel à la transmission de messages, une méthode d'adressage performante à l'intérieur d'un même service;
- le contrôle de la réception, afin que l'utilisateur puisse s'assurer, au moyen d'un système de numérotation des paquets, d'avoir reçu toute l'information;
- et enfin, l'extension du protocole de la voie d'identification des services afin d'accommoder le grand nombre de services de données pouvant coexister dans le multiplex et afin de fournir la description nécessaire à l'interprétation(*).

Les idées et expressions des fonctions requises ont été ensuite affinées pour aboutir à des définitions suffisamment détaillées que pour être transposées immédiatement en structures de codage et fonctions supportées par le protocole de transport.

3. L'accès conditionnel et le protocole de transport de données

Le principe régissant les méthodes d'accès conditionnel définies pour les standards MAC/paquet, repose sur la définition d'une hiérarchie de clés, utilisées pour définir les groupes d'utilisateurs autorisés à recevoir un service, le niveau le plus élevé servant à transmettre le mot de contrôle permettant le désembrouillage (voir figure 1). Ces mots de contrôle sont changés à intervalles réguliers, approximativement toutes les 10 secondes. Les mécanismes, définis au départ pour les composantes traditionnelles (image, sons et télétext), peuvent être étendus et utilisés pour chaque service de données dont l'accès doit être contrôlé.

Les mots de contrôle et les clés d'autorisation sont transmis aux utilisateurs en utilisant une partie de la capacité du multiplex paquets. C'est ainsi que la transmission des clés d'autorisation d'un service requiert un nombre de paquets proportionnel à la taille du groupe à définir; tandis que les besoins en capacité pour la transmission des mots de contrôle sont fixes dans le temps, pour toute la durée d'un service. On voit donc que la capacité supplémentaire, requise par service, pour l'accès conditionnel est directement liée à la taille du groupe d'utilisateurs. Donc ces systèmes seront particulièrement adéquats pour les services ayant une durée de vie, ou une quantité d'information à transmettre relativement importante. En effet, dans ce cas le nombre de paquets nécessaires pour transmettre les autorisations sera une faible fraction du nombre total de paquets transmis pour ce service. Par contre dans le cas des services envoyant de courts messages à des groupes, même restreints d'utilisateurs, le rendement d'utilisation du canal pour les données diminuera d'autant plus que le message sera court.

Ceci devient d'autant plus critique, que le nombre de services opérant simultanément de la sorte augmente. Cependant cette contrainte reste vraie pour tout système utilisant le canal de transmission pour la définition dynamique d'un groupe d'utilisateurs.

Une autre limitation inhérente aux systèmes d'accès conditionnel définis pour le MAC/paquet est l'impossibilité de modifier l'autorisation d'accès à un autre moment que celui du changement de mot de contrôle (toutes les 10,24 secondes). On voit donc que pour les services de type transmission de messages, le système d'accès conditionnel devra être complété par un autre mécanisme permettant, pour l'adressage, une résolution au paquet près. Ceci est rendu possible grâce au protocole de transmission défini pour les services de données.

(*) NOTE: L'approbation du protocole pour l'extension de la voie d'identification des services est actuellement en cours de réalisation au sein de l'U.E.R.

Le système de transport défini pour les services de données repose sur la structure de paquet déjà existante: paquet de 751 bits dont les 23 premiers constituent l'en-tête fournissant l'adresse du paquet, suivit de l'octet PT décrivant le type du paquet, les 720 bits restants formant le champ disponible pour les données. Le type de paquet distingue les paquets d'information embrouillés, ou non, et les paquets d'interprétation. Dans le cas le plus général, les 720 bits ou 90 octets sont disponibles pour la transmission; et la correcte interprétation des données repose sur un accord préalable entre source et réception. D'autres mécanismes offrant plus de flexibilité ont également été définis (voir figure 2).

Un second en-tête facultatif et de longueur variable peut être utilisé au début du champ de données pour tous les paquets d'un service. Le premier octet de l'en-tête (FD) est un descripteur de format indiquant lesquelles des fonctions possibles sont utilisées pour la transmission. Les options disponibles sont les suivantes:

- une extension d'adresse de longueur variable permettant de définir des sous-entités au sein d'un même service. Le second niveau d'adressage peut être utilisé pour la transmission de messages. Dans ce cas, l'adresse étendue est égale à l'identification d'un utilisateur ou d'un groupe d'utilisateurs. Alternativement, cette adresse étendue peut différencier différents sous-services au sein d'une même transmission;
- un compteur de paquets (SC) permettant à l'utilisateur de vérifier la continuité et l'absence éventuelle d'une partie de l'information. Le compteur de paquets suit immédiatement l'extension d'adresse, ou en l'absence de cette dernière l'octet FD;
- une longueur de segment (SL) indiquant la longueur de l'information transmise lorsque celle-ci ne remplit pas un paquet complet.

La combination des méthodes d'accès conditionnel et de l'extension d'adresse fournit la flexibilité demandée pour les services de messagerie. L'accès conditionnel limite l'accès au service pour l'ensemble de tous les utilisateurs et groupes d'utilisateurs recevant des messages, tandis que l'adressage d'un message, destiné à une fraction seulement des abonnés au service, s'effectue au moyen de l'adresse étendue définie dans le protocole de transport. L'introduction de nouveaux abonnés au service s'effectue d'abord au niveau de l'accès conditionnel avant de pouvoir transmettre un message aux nouveaux venus.

Dans le cas d'un message destiné à un utilisateur unique, l'adresse unique définie pour l'accès conditionnel peut être réutilisée comme adresse étendue dans chaque paquet. Les adresses de groupes d'utilisateurs peuvent être connues à l'avance, par souscription, ou bien chargées dynamiquement via un paquet d'interprétation adressé à chaque membre d'un nouveau groupe. Lorsque les adresses sont connues à l'avance, cela permet de s'affranchir du surplus de transmission nécessaire à la création d'un groupe.

Lorsque les groupes sont créés dynamiquement, le surplus de transmission devient comparable au surplus généré par l'accès conditionnel. Cependant les temps de réponse restent inférieurs à ceux nécessaires pour le traitement des messages d'autorisation par le module d'accès conditionnel. Une sélection basée sur l'adresse étendue permet, si nécessaire, de changer de destinataire à chaque paquet.

Cependant l'utilisation de l'adresse étendue ne fournit pas le même degré de sécurité que les mécanismes d'accès conditionnel. En effet, tous les abonnés d'un service peuvent théoriquement avoir accès à tous les messages, même ceux qui ne leur sont pas destinés. Lorsque cet effet devient par trop critique, il reste toujours la solution d'embrouiller les données au niveau de chaque message. En général la combination de ces deux mécanismes fournira toute la flexibilité nécessaire pour la transmission des services de données suivant de nombreux scénarios d'opération.

4. Architecture et implémentation d'un récepteur de données opérant en norme MAC/paquet

Un récepteur de données en norme MAC/paquet est constitué de deux ensembles. Le premier effectue la réception du signal et son traitement suivant les protocoles MAC/paquet. Le second interprète les données reçues en fonction d'un protocole d'application et restitue l'information à l'utilisateur.
Certains récepteurs seront dédiés à une seule application alors que d'autres pourront supporter plusieurs applications différentes. Ces derniers seront implémentés autour d'un ordinateur personnel (de type PC) qui contrôlera la réception du signal MAC, l'extraction d'un ou plusieurs services et supportera le traitement des données par différents logiciels d'applications. Un ordinateur personnel autorise une approche modulaire des applications supportées par simple ajoute de logiciel et offre un maximum de flexibilité dans l'allocation et l'utilisation des ressources.

La configuration d'un récepteur de données est présentée à la figure 3. Elle comprend:

- une antenne à 12 GHz avec la conversion en fréquence intermédiaire;
- un récepteur et démodulateur, pouvant éventuellement être intégrés sur la carte de décodage MAC/paquet;
- le décodeur MAC/paquet, supportant les standards D et D2, remplissant toutes les fonctions relatives au traitement du protocole de transmission des données. Ce décodeur est développé sur une carte connectée à un des ports d'extension du PC;
- l'ordinateur personnel, contenant la carte spécifique pour le MAC et servant d'interface avec l'utilisateur pour le contrôle du terminal et la sélection des services de données. Le PC effectue également le traitement des données suivant les différents logiciels d'application disponibles;
- les données, une fois traitées, sont restituées à l'utilisateur sur des périphériques adaptés aux types d'applications supportées.

L'architecture et la réalisation de la carte d'interface opérant les fonctions spécifiques du protocole MAC requiert une attention toute particulière. En effet, le traitement et l'interprétation du protocole MAC doivent s'effectuer en temps réel pour des données arrivant en salve, pour le mode normal, ou en continu, dans le cas du plein canal, à 10,125 ou 20,25 Mbps (respectivement D2 et D MAC).

La sélection de l'adresse de paquet, le désembrouillage lié à l'accès conditionnel et le filtrage basé sur l'adresse étendue de paquet s'effectueront en séquence pour chaque paquet arrivant dans le récepteur comme représenté à la figure 4. Un mécanisme de stockage intermédiaire entre les fonctions MAC et le bus du PC doit être prévu car le nombre de paquets et/ou messages destinés à un même utilisateur peut varier jusqu'à atteindre la pleine capacité du canal. En effet, l'état actuel de la technologie des PC ne leur permet pas d'absorber indéfiniment des données à 20,25 Mbps, alors que la carte d'interface, elle, doit pouvoir maintenir ce rythme de travail. La carte d'interface supporte également le module d'accès conditionnel soit via un interface vers un module externe, soit intégré à même la carte (circuit spécifique ou lecteur intégré de cartes à microprocesseur).

5. Conclusions

La réception de données transmises suivant le standard MAC/paquet est un domaine en pleine évolution. L'extension des protocoles MAC ainsi que le développement de terminaux pour la réception permettront la démonstration des possibilités de tels systèmes.
La combinaison des différents mécanismes offerts par les systèmes d'accès conditionnel et les différents modes d'opérations du protocole de transport permettent de couvrir tous les types et scénarios de services de façon performante.
L'introduction des cartes à microprocesseur pour le contrôle de l'accès autorise l'utilisateur à opérer un terminal dans la totalité de la zone de couverture du satellite simplement en introduisant sa carte dans le module de lecture. Ceci permet d'ajouter la notion de transportabilité à la gamme des possibilités offertes aux utilisateurs.

6. Remerciements

Le système de diffusion de données en norme MAC/paquet décrit dans ce document est le résultat du travail de nombreuses personnes. Les résultats furent obtenus grâce aux efforts de l'Union Européenne de Radiodiffusion pour la définition d'une approche commune, à la compagnie "British Satellite Broadcasting" pour leur aide dans la préparation des propositions de protocoles et finalement aux industries Européennes participant au développement des terminaux de réception de données.
Des remerciements tout particuliers sont à adresser à MM H.-H. Fromm et W. Vleeshhouwer de l'Agence Spatiale Européenne pour leur participation active et leur aide apportée à la rédaction de ce document.

7. Références

[1] Specification of the systems of the MAC/packet family - Tech 3258.
EBU, October 1986.

[2] Spécification du système D2-MAC/paquet.
TDF, septembre 1985.

[3] EUROCRYPT Système d'accès conditionnel pour la famille MAC/paquet (version 2).
CCETT, le 4 novembre 1988.

[4] EUROCRYPT Scrambling and Conditional Access System.
EBU - GT V2/SPEC 1049 (Issue 2), 21st October 1988.

[5] General Purpose Data Services within the packet multiplex, DRAFT part 4C for revised version of Tech. 3258 [1].
EBU - GT V2/SPEC 1080.

[6] A low cost receive terminal for MAC/packet data broadcasting.
V. Larock & A.L. Buelens. Proc. Olympus Utilisation Conference, Vienna pp. 19-24.

[7] Data Broadcasting by Stellite.
H.-H. Fromm & B. Salkeld (to be published).

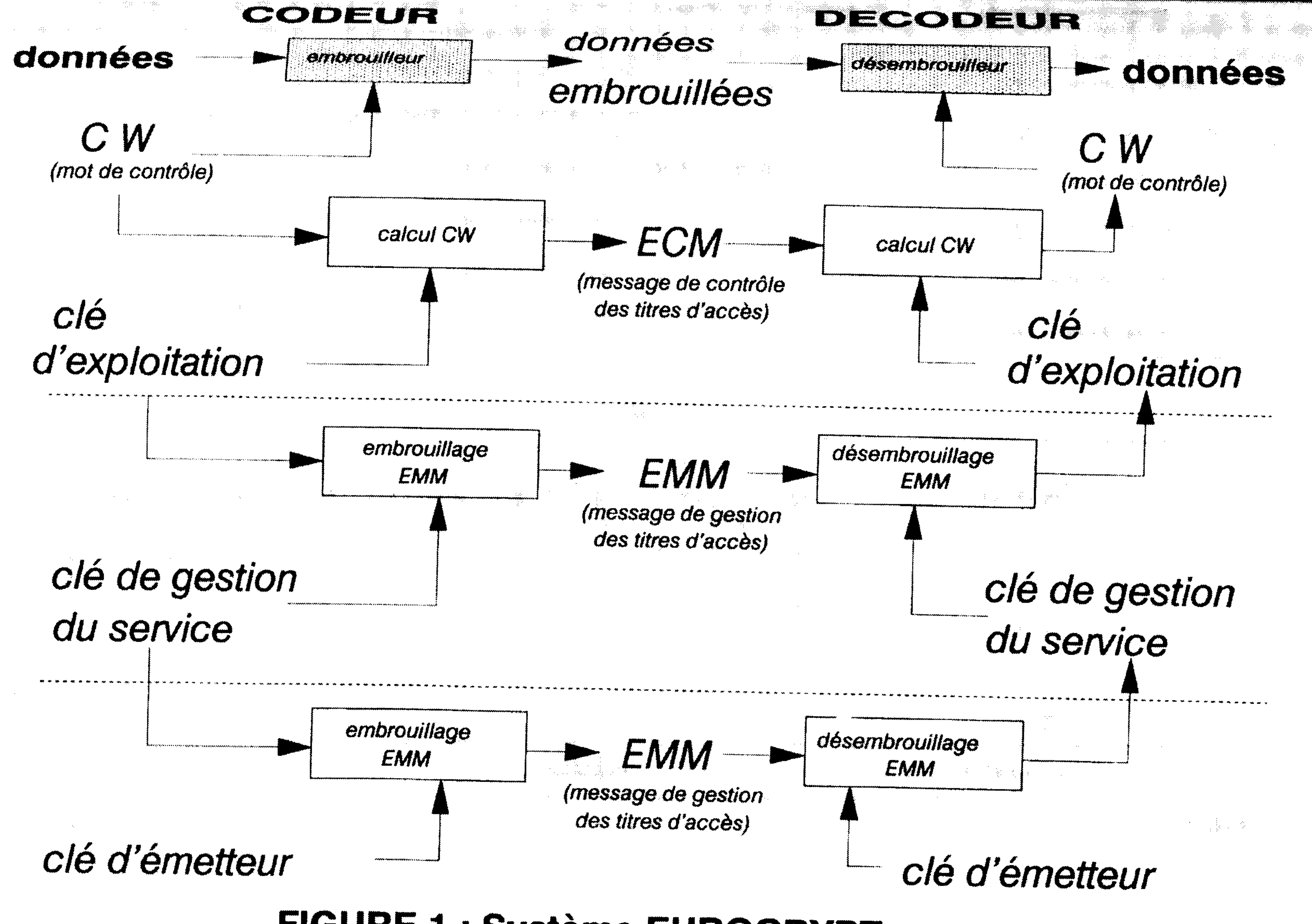


FIGURE 1 : Système EUROCRYPT.

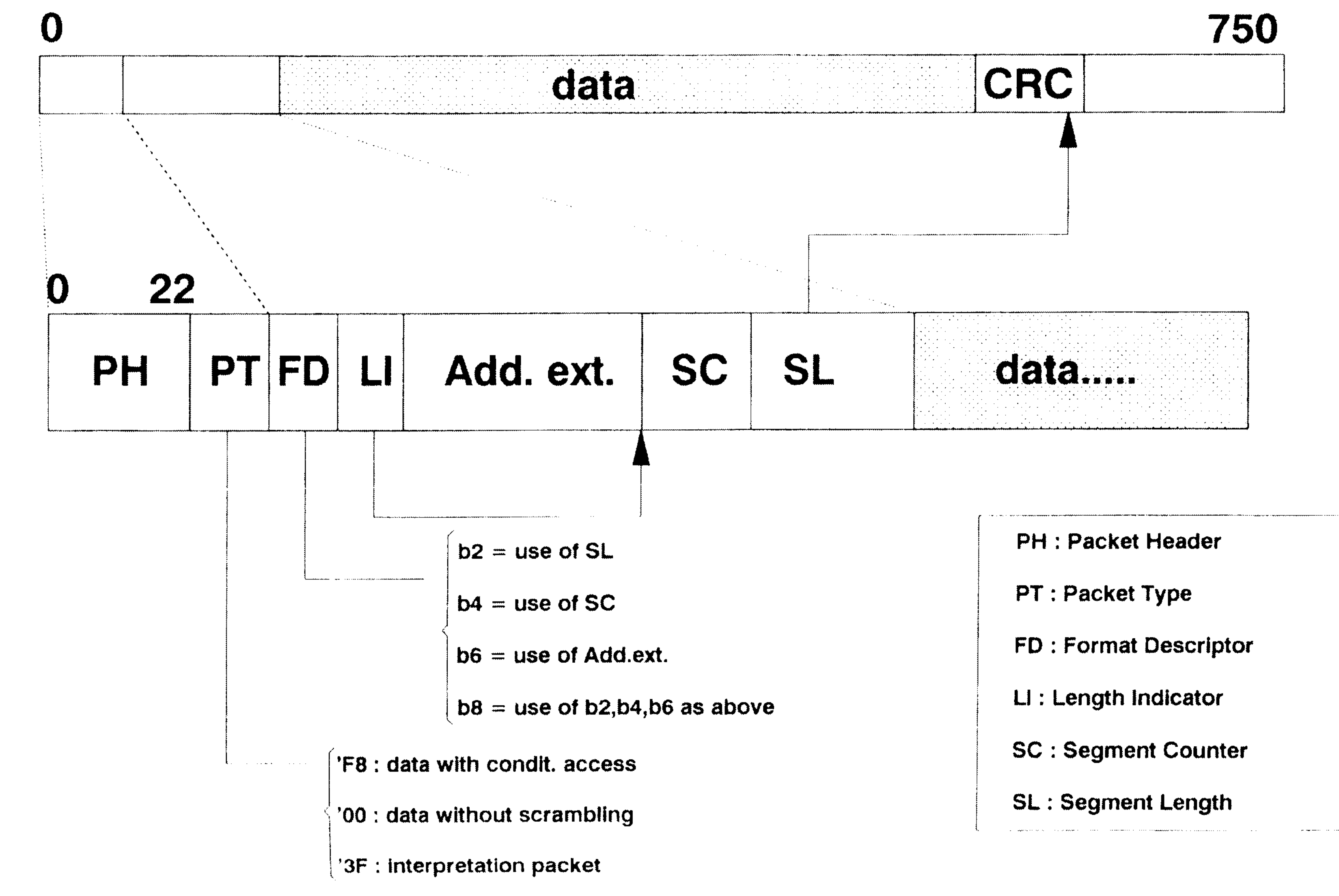


FIGURE 2 : Structure de paquets pour les services de données.

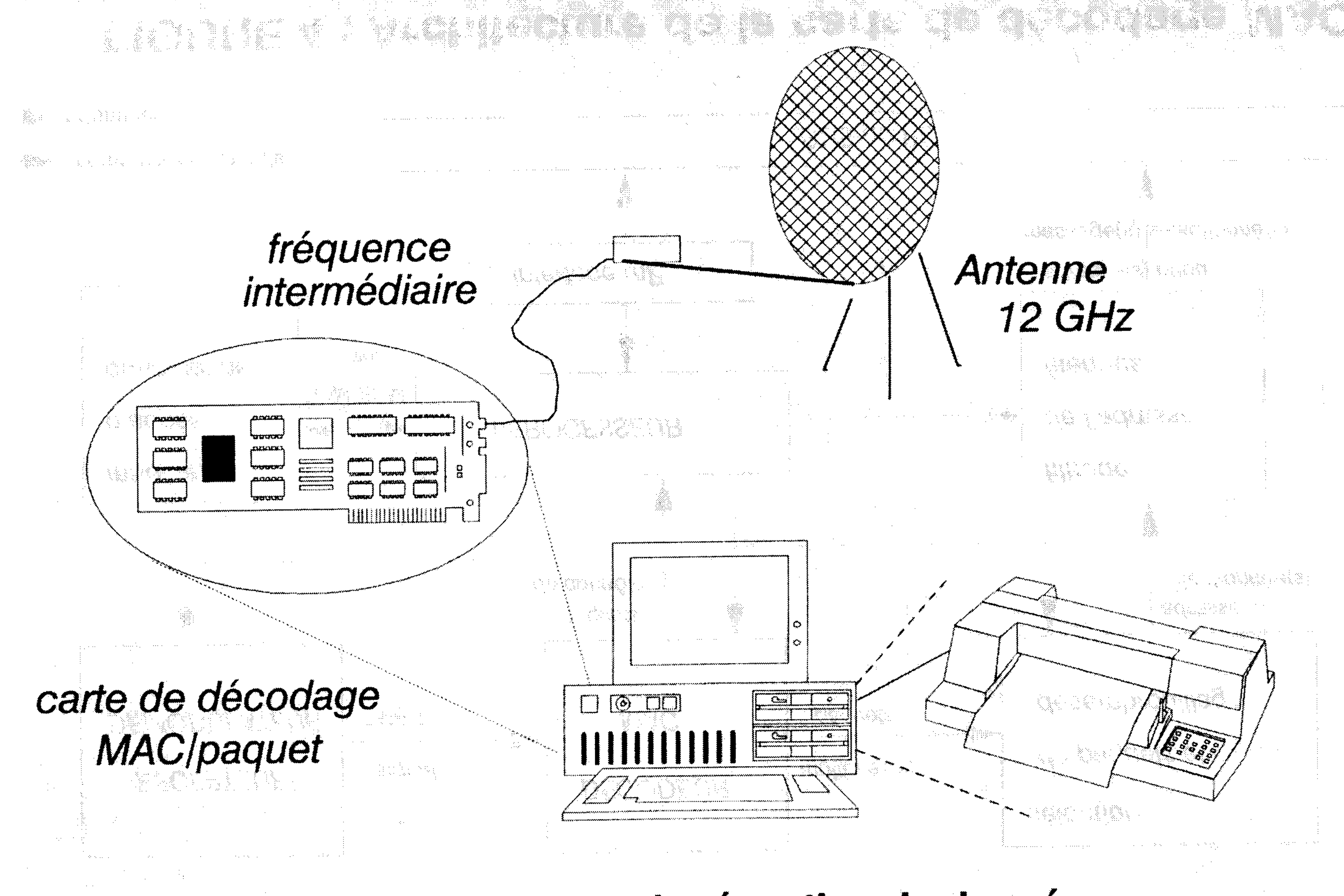


FIGURE 3 : Installation de réception de données.

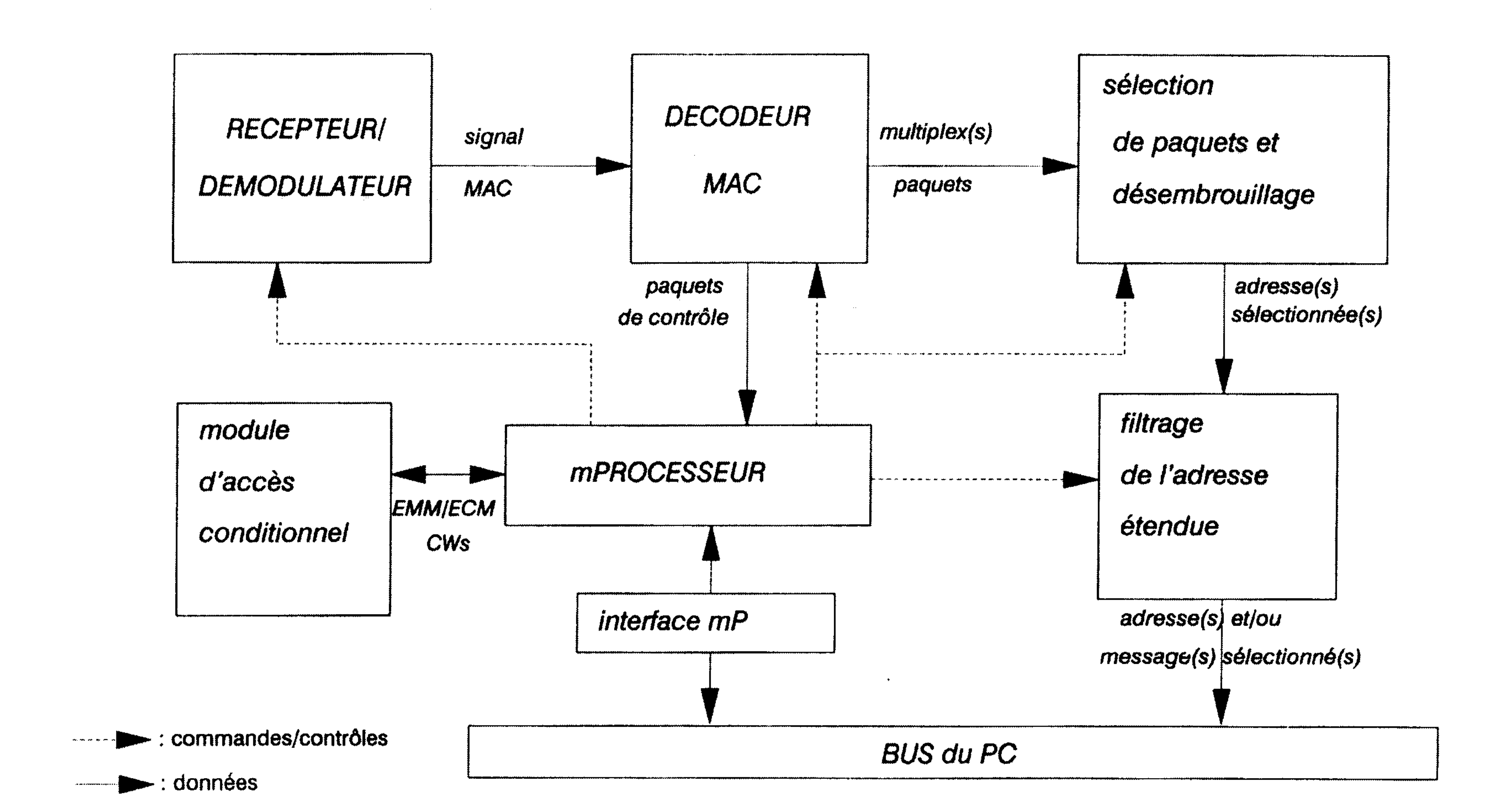


FIGURE 4 : Architecture de la carte de décodage MAC.

EUROCRYPT-S SMART CARD

FOR MAC/PACKET TELEVISION

Ole **HANSVOLD**
Norwegian Telecom Administration
PO BOX 83
2007 KJELLER
NORWAY
Tél : +47 6 809859

Njård **HESTNES**
NORDIC VLSI
PO Box 79
7079 FLATÅSEN
NORWAY
Tél : +47 7 986211

ABSTRACT

This paper presents two security modules designed for conditional access of MAC/packet transmissions. The implementations are based on the Eurocrypt-S conditional access standard. The first generation security module includes all modes and functions specified in the standard. It has been a valuable tool for verification of Eurocrypt-S. However, this component is relatively expensive, so it is likely to be used only in cable-head receivers and other professional equipment.
In order to get a security module tailored for the consumer market a Smard Card version has been developed. The Norwegian Telecom Smart Card offers basic subscription modes a well as the more advanced "impulse-pay-per-view" option. It can serve up to 20 independent scrambled services, and up to 10 independent programm providers. In addition to its high security level it also incorporates a general interface with a powerful user-card dialogue.

TABLE OF CONTENTS

1. Introduction

Norwegian Telecom has been a pioneer in the use of MAC services :

- In 1984 Norwegian Telecom started the first regular MAC transmissions in the world, including both a TV and several sound services.
- Currently Norwegian Telecom operates three D-MAC channels. The Eurocrypt-S/NR-MSK conditional access system is used to control the access to two of them, the Swedish Kanal 1 and TV2. Norwegian Telecom collects subscription fees for access to these channels.

Norwegian Telecom has established a commercial subsidiary, NOTEKA, in order to manage the subscribers for these channels. NOTEKA offers customer management to all program providers who want to use its infrastructure.

The Nordic national broadcasters and the Nordic telecommunications adminstrations, including Norwegian Telecom, have been much involved in the specification of the Eurocrypt-S/NR-MSK conditional access system for MAC.

Norwegian Telecom and the Norwegian companies Nordic VLSI, Tandberg Telecom and ELAB-RUNIT have also been pioneers in the development of MAC system components :

- Three custom VLSI circuits tailored for consumer C/D/D2 MAC receivers. The chipset is marketed by Philips Component and Plessey Semiconductor. The chips are known as the "Philips/Plessey/Nordic chipset".
- C- and D-MAC receivers. The D-MAC receivers incorporate the Eurocrypt-S conditional access system. The receivers are marketed by Tandberg Telecom.
- A first generation Eurocrypt-S/NR-MSK conditional access sub-system (CASS). This is the security module for a conditional access MAC receiver. The security modules are marketed by Norwegian Telecom.
- A MAC encoder incorporating conditional access. The encoders are marketed by Tandberg Telecom.
- A system for administration of subscribers in a conditional access system. The customer management system will be marketed by KVATRO of Norway.

These components together form a complete system for conditional access of MAC transmissions. Current activities aim to upgrade the system to be able to administer very large subscriber populations. Some of the activities are :

- Development of a cheap Smart Card security module for Eurocrypt-S/NR-MSK. Prototypes are ready from the manufacturer this summer, volume production is planned soon thereafter. The cards will be marketed by a Norwegian Telecom subsidiary.
- Development of a distributed system for management of subscribers.

2. Architecture of a MAC receiver incorporating conditional access

MAC receivers with conditional access should satisfy some particular requirements.

2.1 Open receivers

Open receivers implies that the consumer may subscribe to any conditional access service, i.e. the receivers are not limited to a specific program provider. The receiver designs should be based on a standardized open specification so that receivers can be produced by any receiver manufacturer in order to avoid that one manufacturer obtains a monopoly position.

The early scrambling systems have in general provided a low security level and they have neither been flexible nor compatible. This is one of the reasons for the slow development of the satellite-TV/pay-TV market as the public awaits the systems to become more standardized.

The development of a standardized open system MAC receiver which allows the consumer to freely select his programmes is a most important factor for the satellite TV industry to reach its potential.

2.2 The basic receiver

A MAC-receiver consists of three main parts; the transmission system, the descrambling system and the decryption/entitlement checking system.

The MAC transmission- and descrambling systems are standardized. They can therefore be gathered in the same box, the basic receiver. This represents no security risk provided that the complexity of the scrambling is adequate, i.e. it must be infeasible to make cheap devices which are capable of descrambling the scrambled signals without authorised control information.

The basic receiver receives scrambled or open access baseband vision and data signals. It outputs descrambled RGB vision, sound and data signals. The basic receiver has also interfaces towards the security module which performs decryption/entitlement checking, and the user (screen and remote control).

The information that is sent from the basic receiver to the security module are data-packets (SMM, CMM or ECM, EMM). The security module will return the control words necessary to descramble a service provided that it contains the appropriate decryption key and entitlement. The security module may, based on the content of the packets, impose replacement/blackout of a service or fingerprinting of the picture to take place. It will also provide packet-addresses for the basic receiver.

The user interface should, in addition to channel selection, teletext and various control functions, also include communication with the security module in order to enable the user to check his entitlements, dates for when his subscription expires, token status, etc.

The basic receiver may have an identity in order to get a more secure country-by-country control. However, this identity scheme should not limit the basic receiver to a specific program provider, i.e. close it.

2.3 The security module

The decryption/entitlement checking system requires a high level of security, i.e. it should neither by physical nor logical means be possible to extract decryption keys or manipulate entitlements. A very flexible solution is obtained if the decryption/entitlement checking system resides in a cheap separate security module. Whereas the basic receiver is expected to be compatible for a long time, a cheap detachable security module allows the decryption/entitlement checking system to be upda-

ted with better or different functionality more often. This solution is also flexible in the sense that it allows the consumer to attach any standard security module containing entitlements for any channel to his basic receiver.

3. First generation Eurocrypt-S security module

Norwegian Telecom and Nordic VLSI have, based on the Eurocrypt-S standard for conditional access of MAC/packet transmissions, developed software for two security modules.

The first complete Eurocrypt-S security module was ready in June 1989 . Its software includes all modes and functions specified in the standard.

The simplest mode of Eurocrypt-S is denoted "Static subscription". Its main advantages are simplicity, minimum data overhead (no SMMs or ECMs are transmitted), and support for many independently scrambled services. The disadvantages are no replacement/blackout facility and no date checking. Static subscription is simple both to install and to operate on the transmission side. It is also suitable for PAL encryption systems.

All other modes use Service Management Messages (SMM or ECM) to send the control words needed for descrambling. "Dynamic subscription" is the most flexible mode which offers a wide range of possibilities including subscription per service element, e.g. subscription to sports and news but not films in a channel, "pre-booked programme", "impulse pay-per-view", etc. This mode covers most modes of the Eurocrypt-M standard. The "Turbo dynamic subscription" mode reduces the storage requirements in the security module at the expense of more Customer Management Messages (CMMs or EMMs) in the MAC-packet multiplex.

"Impulse pay-per-view" (IPPV) use tokens inside the security module to pay for the programs. Programs may be bought per time unit (10 sec) or per program. The price of a program is defined by the program provider. Token store in the security module can be updated over-the-air or by other means.

The software was implemented in a DS2250 MCU from Dallas Semiconductor. The DS2250 incorporates 32Kbytes of battery backed RAM, and an Intel 8051 compatible CPU running on 12MHz, so it is a relatively powerful MCU.

The DS2250 implementation has served as a valuable debugging tool for the Eurocrypt-S specification which now is fully verified. It has also been vital for testing the Tandberg Telecom encoder equipment as well as the complete conditional access system. The test setup was complete with encoder, satellite-link and decoders located several places in Europe under different climatic conditions. The duration of the test period was more than a year.

The MAC receivers made by Tandberg Telecom contain the DS2250. These receivers are in daily use, mainly by cable network operators in Norway and Sweden.

The main disadvantage of the DS2250 is that it is expensive for the consumer market. However, for cable-head receivers and other professional equipment it is a good and available alternative.

4. Second generation Eurocrypt-S security module, the Norwegian Telecom Smart Card

In order to get a more cost effective security module, the DS2250 software has been modified to be run on a Motorola MC68HC05SC21 Smart Card MCU. The -SC21 has 6Kbyte of ROM and 3Kbyte of EEPROM. The core Eurocrypt-S functions reside in ROM, while enhanced functions can be loaded into EEPROM. This makes it easy to tailor the card for specific requirements.

4.1 Interface

The format of the Norwegian Telecom Smart Card and its contacts conforms with the ISO 7816 standard for Smart Cards. The card also incorporates the transmission protocol specified in ISO 7816.

The application protocol, i.e. the application data being transported by the transmission protocol, is very powerful and as simple as it can possibly be. Eight commands are defined, only one of these are Eurocrypt-S specific, the others can be used to communicate with a Eurocrypt-M or a Eurocipher card. This general approach is therefore a step towards making the basic receiver more transparent for the encryption system.

The basic receiver sends complete packets (SMM, CMM or ECM, EMM) unprocessed to the card, i.e. the only concern of the basic receiver is to pick out the right packets and send them to the card. As a result of the processing of a packet the card returns control words for the descramblers, replacement or fingerprinting information and/or text to be displayed on the screen.

The application protocol also incorporates a powerful user-card dialogue. The card, rather than the basic receiver, supplies menus to be displayed on the screen. Selections made by the user which concern the card are not interpreted by the basic receiver, thus making the user-card dialogue independent of the specific receiver implementation. The basic receiver is just a transmission medium for the information being exchanged.

The mechanism allows new menus to be issued with new card generations. This is particularly useful for the customer management as they will only have one set of menus to relate to when they get inquiries from the users. On the other hand, if the menus are different for each receiver manufacturer and each receiver generation, the task of guiding a subscriber through a set of menus becomes more time consuming.

The user-card dialogue also allows the different program providers to define their specific menus, or specific information e.g. their new telephone number or an advert, to be put into the cards. Cards with menus in the appropriate language can be issued in different countries.

The fact that all the processing of the packets takes place in the card and that the menus for the user-card dialogue are provided by the card makes the basic receiver easier to implement.

4.2 Conditional access functions in ROM core

The ROM program in the Norwegian Telecom Smart Card includes the Eurocrypt-S functions "Dynamic subscription", "Static subscription", replacement/blackout and fingerprinting determined by geographical location or other criteria, and addressed teletext messages to individual users or groups of users.

4.3 Enhanced functions which can be loaded into EEPROM

The Norwegian Telecom Smart Card have a programming function which allows additional commands and conditional access functions to be loaded into the EEPROM. These enhanced functions include "impulse pay-per-view " per time unit or per program, viewing history function to be used in conjunction with pay-per-view in which the card stores program numbers which can be dumped when the card is reloaded, and user menus.

It should be noted that "impulse pay-per-view" requires non-volatile memory (e.g. EPROM or EEPROM) for secure operation. "Impulse pay-per-view" per time requires that the "token-tank" kept in non-volatile memory is charged every 10th second. EPROM can only be written once when

embedded into a card, so with current technology only cards containing EEPROM can be used for this subscription mode.

Also special functions required by a program provider can be developed and put into EEPROM.

4.4 Security features

The security module must incorporate secure storage of program and data, and secure execution of its software. The security aspect can be divided into logical security and physical security.

Logical security includes issues like the security level the crypto-algorithm provides and secure programming, i.e. insure that it is not possible to manipulate the card to reveal any of its secrets by giving it unauthorised input.

All communication of sensitive information to and from the Norwegian Telecom Smart Card is encrypted, thus keys never exist in plaintext outside the card. Fusible links permanently prevent access to the manufacturing test mode. The ROM or EEPROM contents can therefore not be dumped on the communication port undeliberately.

Physical security includes techniques which are used to resist attempts to exhaust secrets by physical attacks like probing and use of electron-microscope. The Norwegian Telecom Smart Card has a high level of physical security. It contains a single chip micro-controller unit (MCU) which is a chip with CPU, I/O, program and data memory all on a single piece of silicon. No external buses exist except for a serial I/O line controlled by the internal program.

The internal buses are less than 2 micrometer wide, and therefore only very sophisticated equipment may be able to tap these buses. In order to access the buses at all a so-called passivation layer must be removed successfully by chemical etching.

All keys and entitlements are stored as charges in EEPROM. The MCU also have special security features like low frequency detection to insure a certain speed on the internal buses, low power detection, etc.

4.5 Card economy

Single chip MCUs designed for security applications offer the optimum trade-off between security, functionality and price. They are therefore well suited for consumer applications in which security is an issue.

In order to obtain the most cost-effective solution the same card should be shared between several program providers. This is not always easy to achieve in practice as program providers are competitors. However, co-operation between program providers in non-conflicting markets are likely, it will also be established customer management organisations which provide the infrastructure for management of customers on behalf of many program providers, e.g. program providers who prefer to have a small organisation, and program providers whose position in the market in a particular area makes it inprofitable to maintain their own customer management there.

The Norwegian Telecom Smart Card can serve up to 20 independent scrambled services, and up to 10 independent program providers.

The Norwegian Telecom Smart Card has dynamic allocation of EEPROM data memory. This means that a key or an entitlement may be created and erased as appropriate, i.e. the card can be reused. This is an advantage for the card issuers as the cards will not have to be replaced as often as EPROM cards.

The Norwegian Telecom Smart Card can be updated over-the-air or via terminal. Infrastructure for

initialisation/reloading of cards via terminal are now being developed by the Norwegian Telecom.

5. Future security modules

As the market develops there will probably be demand for both very low cost cards which contains entitlements for just a particular event, e.g. the Olympic Games, and for advanced cards which allow the program providers to run very flexible services.

Future products from Norwegian Telecom will include useful subsets of the DS2250 and the -SC21 implementations. By having complete implementations of the Eurocrypt-S running on the most popular Smart Card MCU cores (8051 and 6805) new products which meet certain demands can easily be developed.

Generic cards may also be developed, but for the moment the advanced pay-TV applications tend to use all the memory available in the MCUs.

CONDITIONAL ACCESS FOR OFF-AIR
AND LOCAL GENERATED PROGRAMMES
IN CABLE TV NETWORKS

Helge STEPHANSEN
Tandberg Telecom a.s.
Box 333
1473 Skårer
NORWAY
Tél : +47 2 973170

ABSTRACT

The portion of television viewers who get their programmes by cable is large and steadly increasing. Cable networks need special consideration when implementing conditional access. The cable operator is interested in how business will be affected by the increasing use of scrambling for satellite broadcasting. Likewise the programme provider will be affected by how his signal is handled in cable networks, especially if there are any security risks. At present there are three options for encrypted signals in cable networks : decrypt at the head end, distribute the encrypted signal transparently without changing the scrambling, or re-encrypt the signal with another system. TANDBERG Telecom make MAC receiver/decoders for this signal processing. More advanced units are described, e.g. equipment that can multiplex entitlements for the cable network into the off-air MAC signal.

RÉSUMÉ

Le nombre de téléspectateurs qui reçoivent leurs programmes par câble est déjà considérable et augmente toujours. Les réseaux câblés ont besoin de considération particulière quand on introduit l'accès conditonnel. L'opérateur de câble s'intéresse à la façon dont est touché le marché par l'utilisation plus extensive de brouillage pour une diffusion par satellite. Le fournisseur de programme sera aussi touché par la manière dont son signal est traité dans le réseau câblé, particulièrement s'il y a des risques de sécurité. À présent il y a trois possibilités pour les signaux cryptés dans les réseaux câblés : décrypter la tête, distribuer le signal crypté de façon transparente sans changer le cryptage ou recrypter le signal avec un autre système. Des unités plus avancées sont décrites, par exemple des équipements qui injectent les autorisations particulières pour le réseau câblé dans le signal MAC reçu par air.

TABLE OF CONTENTS

CONDITIONAL ACCESS FOR OFF-AIR AND LOCAL GENERATED PROGRAMMES IN CABLE TV NETWORKS

Helge Stephansen, Tandberg Telecom a.s., Skårer, Norway
Tel. +47 2 97 31 70

1. Introduction

Encryption of television was introduced in cable networks to earn revenue from locally-inserted programmes such as movies. At that time the programmes available off air were transmitted in clear and could be freely accessed by anyone. Of course in some countries an annual subscription fee is imposed for the national programme(s). In recent years this situation has changed. More and more satellite and terrestrial television channels are encrypted. This serves two purposes, one is to protect the signal against reception outside the area for which rights have been acquired and the second purpose is to gain income from subscription and pay-per-view services. Access control will play an important rôle in satellite broadcasting due to the large audience able to pick up the signal, and will continue to be valuable for terrestrial broadcasting.

1.1 Cable Networks

Cable networks are an efficient means of feeding many television programmes to a large number of viewers. Cable networks are increasing in size and number and will carry more and more channels to more and more subscribers. The networks range from small master antenna networks to large ones with around a hundred thousand outlets. The small networks can not afford to set up their own customer management systems so they are restricted to relaying the signal received off-air. For the large networks, however, the cost of a subscriber management set-up can be justified as the number of subscribers creates a viable market.

The majority of viewers of satellite-transmitted signals are connected to a cable network. They need special consideration in connection with encryption of programmes and conditional access systems.

I will give a description of the situation as it may be seen by the cable operator and by the programme provider. However, I represent neither of them so my description may be incomplete or imprecise.

1.2 Significance of Conditional Access in Cable Networks ...

1.2.1 – for the Cable Operator

The cable operator gains his revenue from distribution of programmes to his subscribers and conditional access is a means to provide a flexible delivery to them. The customers can subscribe to the channels they want to view, and those without subscriptions are denied access to these programmes. The cable operator can thereby increase his income.

Accordingly the cable operator wants complete control of his customers' subscriptions, and as a minimum an income for distribution of any channel, scrambled or not.

Many cable networks transmit locally-generated channels in addition to the channels received off air. To restrict access to these channels encryption is necessary, and a customer administration function has to be set up. To make this attractive to subscribers a single decryptor unit must accept all the channels in the network. A good solution for the cable operator can be to rescramble all channels with his own conditional access equipment.

Let our cable operator choose to use D/D2-MAC [1] as this standard will be widely used in the coming decades. A conditional access system is applied to encrypt his channels and the ECM/EMM - SMM/CMM messages [2]. He wants access to his local channels to be quick so he inserts his EMM/CMM in all the MAC channels in the network. Still better, he may replace the original EMM with his own or even rescramble the signal to gain selective control of his subscribers. For these last two options it is necessary to have an agreement with the original encryption organisation.

In all cases the programme provider is dependent on the cable operator for the distribution of the programme in the network.

1.2.2 – for the Programme Provider

For the broadcaster the cable networks represent a large number of potential customers and hence income. However, if the signal is decrypted at the head-end, a cable network may represent a large number of unauthorized viewers outside his control. As any decoder/decryption unit can be used as easily in a head-end as in a domestic home it may be easy to cheat the programme provider. The only ways to restrict the use of decoders are by legislation or agreement, which are impractical on an international scale since nations' broadcasting laws differ.

From a security viewpoint, broadcasters are less likely to allow the insertion of new EMM/CMM at cable head-ends as this would mean a spreading of the encryption algorithm unless the central organisation provides EMM/CMM to all cable networks within a region, for instance one organisation for each nation.

In all cases where cable operators follow the rules, the cable operators are dependent on the programme provider to decrypt or re-encrypt the programme.

1.3 Advantage of Cooperation between Cable Operator and Programme Provider

The best solution can only be achieved if the broadcaster and the cable operator cooperate. A solution that may relieve their concerns is as follows.

The cable operator and broadcaster set up an organisation for generating CMM/EMM for the cable networks. Each cable network gets a set of CMM/EMM made up according to all channels subscriptions within the network.

For the locally generated channels this set of EMM/CMM are used. For the off-air channels three possibilities exist: discard them, let them go through or replace them.

2. Equipment for MAC Signals in Cable Networks

At TANDBERG Telecom we are designing a new range of decoders/encoders for use in cable networks:

TT-1020 PROMAC
This receiver has a tuner for the 950–1250 MHz band, a MAC decoder and transcodes to PAL.

TT-1020/07 MAC Regenerator
The regenerator receives FM modulated channels off air and converts them to MAC baseband. Doubinary data are regenerated in order to improve noise and echo margins before feeding the signal into the network.

TT-5000 D-MAC / TT-5100 D2-MAC Cable Encoder
These encoders are low-cost units suitable for cable networks.

TT-5500 MAC Multiplexer
This unit can multiplex the a new stream of packets into an existing MAC/packet signal.

TT-5600 MAC Rescrambler
This unit rescrambles a MAC/packet signal and inserts new ECM/EMM - SMM/CMM packets.

2.1 Receiver and Decoder Equipment

TANDBERG Telecom manufacture two receiver/decoders for use in cable and master antenna networks, *PROMAC* and *TT-1020 MAC Regenerator*. Both units are fully D- and D2-MAC/packet compatible. PROMAC transcodes from MAC to PAL, and the MAC regenerator converts an FM signal to amplitude-modulated VSB (vestigial sideband).

2.1.1 TT-1020 PROMAC

The TT-1020 receives the signal directly at the first IF band 950 - 1750 MHz. The tuner and demodulator are controlled by a microprocessor in order to achieve very low bit error rate and optimum baseband MAC signal. Clamping error is minimised to give a high quality PAL picture free from green or red discolouring.

The decoder has an optional board to handle teletext in the VBI format. The VBI teletext in the MAC signal is converted from doubinary format and inserted into the PAL output signal.

The PAL subcarrier is locked to the line sync signal. This is necessary to avoid interference with possible remnant of PAL carrier that may be present if the input signal has been PAL coded previously.

The TT-1020 can be equipped with internal or external modules for decrypting Eurocrypt S. A smart card interface for Eurocrypt M will be available in 1990.

2.1.2 TT-1020/07 MAC Regenerator

The regenerator receives FM-modulated channels off air from satellite and converts the signal to MAC baseband. Duobinary data are regenerated in order to improve noise and echo margins before feeding the signal into the network. The regenerator is particularly useful where the input signal is weak as the noise-to-carrier ratio of the data signal is increased from a high value to an insignificant one before retransmitting on the network. The video signal is passed through a sophisticated clamp circuit to remove the energy dispersal, and is delayed to compensate for the delay in the data part of the decoder. An optional amplitude modulator may be included in the regenerator.

The regenerator is transparent to the encryption system and can accordingly be used for transmissions with Eurocypher, Eurocrypt M or Eurocrypt S.

2.2 Encoding equipment

TANDBERG Telecom offer a range of MAC/packet encoding equipment. The input is normally a PAL, SECAM or component video signal, but we can also deliver equipment to convert a MAC signal into a modified MAC signal if that is desired. The following paragraphs describe the units in more detail.

2.2.1 TT-5000 Series Cable Encoder

These encoders are low cost solutions for cable networks and wil be available in two versions; one for D-MAC (TT-5000) and one for D2-MAC (TT-5100). Both encoder versions can be used for all encryption system registered by EBU. The philosophy behind the design of the 5000 encoder series is that encoders for cable networks must meet the following requirements:

- reasonable cost.
- easy to use, the encoder must configure as desired at power up.
- it shall be possible to define the default configuration according to customer requirement.
- reliable and easy to maintain.
- alarm raised if a failure occurs or input signal is not present.

The input signals can be either in PAL, SECAM or component video. The basic configuration has one stereo sound channel. Teletext is optional. The output signal is normally baseband MAC, but inclusion of an FM or AM modulator is optional. The System Identification (SI) packets and line 625 high priority SI are generated automatically in accordance with the encoder configuration.

The 5000 MAC/packet encoder family may be configured with hardware modules for generating control words (CW) and entitlement checking messages (ECM), as well as an interface module for entitlement management messages (EMM) for Eurocrypt M. Alternatively the CW and ECM modules can be replaced with interface modules for Eurocrypt S or Eurocypher.

2.2.2 TT-5500 MAC Multiplexer

This unit can multiplex a new stream of packets into an existing MAC/packet signal. The TT-5500 MAC multiplexer is intended to be used by large cable networks who want to insert their own EMM messages into an off-air received MAC signal. These EMM's may represent the entitlements for the complete set of channels for all the subscribers in the network. Note that these EMM's must contain the correct program provider identifier and be encrypted by the provider's algorithm to be of any use. The EMM must accordingly be generated by the programme provider on request from the cable operator. EMM's for different programmes can be multiplexed on a channel.

The original EMM must be removed and the new EMM inserted at the same location in the subframe in order not to violate the scrambling.

A feature of the multiplexer is that it enables the cable operator to participate in the customer administration so he is able to control his subscribers. Furthermore for a subscriber, it greatly decreases the possibility of losing an entitlement for a particular channel which he/she seldom watches as the entitlements for all channels may be multiplexed (integrated) on every channel. The benefit for the programme provider is that the cable operator can act as his local agent.

The multiplexer input signal is D/D2-MAC. The signal can be at baseband, or FM modulated at 70MHz or in the range 950 to 1750 MHz.

2.2.3 TT-5600 MAC Rescrambler

This unit will rescramble a MAC/packet signal and insert new ECM/EMM - SMM/CMM packets. The unit gives the cable operator full subscriber-management control of the outgoing MAC signal. The unit is equipped with an Access Control Module in order to decrypt the incoming signal.

The unit is mainly intended to convert from one conditional access system to another, for example from Eurocrypt S to Eurocrypt M.

References

[1] *Specification of the Systems of the MAC/packet Family*, EBU Tech. 3258-E, October 1986.
[2] C. Bradley & H. Stephansen, *Versatile MAC/packet Encoder Interfacing with any Conditional Access System*, ACSA'90, accompanying this article.

PRÉSENTATION DU TERMINAL D'USAGER

NAGRAVISION / SYSTER

André **KUDELSKI**
Nagravision S.A.
1033 CHESEAUX
SUISSE
Tél : +41 21 731 41 65

RÉSUMÉ

Canal Plus introduit actuellement en France et en Espagne le nouveau terminal d'usager SYSTER. Cet appareil est destiné aux réseaux terrestres des deux chaînes qui sont respectivement exploitées en SECAM et en PAL.
Le terminal SYSTER est appelé à être produit en grande quantité par Eurodec et bénéficie d'une très forte intégration, par la réalisation de circuits intégrés spécifiques.
La mise en exploitation du terminal SYSTER demande l'introduction d'un système d'émission intégré permettant au centre de gestion des abonnés d'intervenir de façon sélective sur les droits d'accès des terminaux, par informatique et embrouilleurs/injecteurs interposés.
Le système NAGRAVISION/SYSTER brouille l'image par permutation de lignes et possède son propre système d'accès contrôlé, tout en assurant une compatibilité ascendante avec le système discret-11, utilisé actuellement sur Canal Plus.

ABSTRACT

The french TV operator Canal Plus is currently introducing in France and Spain a new descrambling terminal (Pay-TV decoder). This terminal will be used on terrestrial networks in both France and Spain.
The Syster terminal is designed to be manufactured in large quantities and is highly integrated by the use of custom made integrated circuits.
The use of the SYSTER terminal requires an integrated management concept, permitting the management computer to selectively modify the access rights of the terminals, through the use of computers and scramblers.
The NAGRAVISION/SYSTER system scrambles the video signal by line shuffling and has its own access control subsystem. It is, however, upward compatible with the current discret–11 descrambling terminal.

DÉSEMBROUILLEUR VISIOPASS

ET ACCÈS CONDITIONNEL

Gérard **DUVIC**
CCETT
4 rue du Clos Courtel
BP 59
35512 CESSON SEVIGNE Cedex
FRANCE
Tél : +33 99 02 41 37

Christian **GEOFFRAY**
La Radiotechnique Portenseigne
Les Patios
24 quai Galliéni
92156 SURESNES Cedex
FRANCE
Tél : +33 (1) 40 99 62 03

ABSTRACT

After a review of a the various functions included in the VISIOPASS terminal, the basic ones for D2 MAC/packet decoding and coditional access are emphasized. Particular attention is drawn to the user interface since product acceptability strongly depends on its design. The various interactions between the terminal and the viewer are described, while stressing the new capabilities provided by the use of D2 MAC/packet and Eurocrypt.

RÉSUMÉ

Après un examen des différentes fonctions du terminal VISIOPASS, l'accent est mis sur les fonctions de base liées au décodage du D2 MAC/paquets et à l'accès conditionnel. Une attention toute particulière est portée à l'interface "téléspectateur", car l'acceptabilité du produit dépend largement de la conception de cette interface. Les différentes interactions entre le téléspectateur et le terminal sont décrites, en soulignant les nouvelles possibilités ouvertes par l'utilisation du D2 MAC/paquets et d'Eurocrypt.

TABLE DES MATIÈRES

ABSTRACT

After a review of a the various functions included in the VISIOPASS terminal, the basic ones for D2 MAC/packet decoding and coditional access are emphasized. Particular attention is drawn to the user interface since product acceptability strongly depends on its design. The various interactions between the terminal and the viewer are described, while stressing the new capabilities provided by the use of D2 MAC/packet and Eurocrypt.

RÉSUMÉ

Après un examen des différentes fonctions du terminal VISIOPASS, l'accent est mis sur les fonctions de base liées au décodage du D2 MAC/paquets et à l'accès conditionnel. Une attention toute particulière est portée à l'interface "téléspectateur", car l'acceptabilité du produit dépend largement de la conception de cette interface. Les différentes interactions entre le téléspectateur et le terminal sont décrites, en soulignant les nouvelles possibilités ouvertes par l'utilisation du D2 MAC/paquets et d'Eurocrypt.

TABLE DES MATIÈRES

1. INTRODUCTION

Dans l'ensemble des moyens mis en œuvre par FRANCE TELECOM pour permettre d'assurer un service de contrôle d'accès pour programmes audiovisuels, le terminal VISIOPASS assure une fonction particulièrement importante dans la relation avec le téléspectateur.

Il permet en effet de répondre aux demandes du téléspectateur qui souhaite utiliser les modes de consommation suivants :

- Consommation à l'abonnement, par thème et par niveau.
- Consommation à l'abonnement par classe.
- Consommation d'émissions télévisées sur réservation.
- Consommation d'émissions télévisées sur décision immédiate, à la séance.
- Consommation d'émissions télévisées sur décision immédiate, à la durée.

Dans les deux derniers cas, la consommation effective ne peut être connue qu'à postériori. Le téléspectateur acquiert en effet au préalable un forfait de "jetons". L'analyse détaillée de la consommation peut être saisie par le Gestionnaire des titres d'accès (GTA) au moyen d'un relevé de "jetons" consommés, grâce au modem dont le terminal est équipé à cette fin.

Le terminal VISIOPASS est conçu pour permettre à la carte PC2, qu'il reçoit dans son lecteur de carte avec volet de protection, d'accueillir des messages de gestion des titres d'accès (EMM) transmis par le réseau de diffusion, en particulier à la suite de requêtes du téléspectateur.

2. FONCTIONS TECHNIQUES ASSUREES PAR LE TERMINAL

2.1. Architecture générale du terminal

On distingue deux types de VISIOPASS :

- Pour le câble où le terminal reçoit des signaux codés en D2-MAC/paquets ou en SECAM. Dans ce dernier cas, le terminal démodule simplement le signal HF et le distribue vers les deux prises péritélévision dont il est équipé.
- Pour la réception directe par satellite où le signal traite exclusivement les signaux HF conformes au plan CAMR 77.

Les configurations d'interconnexion du terminal avec ses périphériques, essentiellement le téléviseur et le magnétoscope sont illustrées sur la figure 1.

La sortie péritel 1 (P1) est la voie normale mais non exclusive de connexion au téléviseur. La sortie péritel 2 (P2) est la voie normale de connexion à un magnétoscope de type VHS, en lecture ou en enregistrement. Dans ce dernier cas, si le programme à enregistrer est de type D2-MAC/paquets, un transcodage en SECAM est effectué, avant sortie du signal sur P2.

La prise P2 permet également un accès en bande de base d'un signal D2-MAC/paquets en provenance d'un syntoniseur extérieur par exemple. P2 permet aussi de délivrer un signal D2-MAC/paquets en bande de base provenant directement du syntoniseur du terminal.

D'autre part, une sortie Hi Fi de type CINCH, permet de délivrer le son associé au programme TV ou un programme radio transporté par un canal D2-MAC/paquets.

La figure 2 illustre l'ensemble des fonctions constituant un terminal VISIOPASS :

- Alimentation (et téléalimentation possible du convertisseur de fréquences).
- Régie audiovisuelle.
- Décodage D2-MAC/paquets.
- Interface d'accès conditionnel.
- Interface téléspectateur.
- Horloge de programmation.
- Modem.
- Démodulation FM (version satellite).
- Démodulation MABLR (version câble).

Certaines de ces fonctions sont présentées plus en détail dans les paragraphes qui suivent.

2.2. Fonctions de base

2.2.1. Traitement du signal D2-MAC/paquets

Le traitement du signal D2-MAC/paquets s'appuie sur l'utilisation du kit de composants ITT, le décodage étant effectué en conformité avec les documents de référence suivants :

- Documents AFNOR NFC 90 001 + NFC 90 001 Additif 1.
- Eurocrypt (mars 89) + règles d'exploitation (2ème phase).

Le terminal permet de décoder un programme TV, avec extraction simultanée de deux sons mixables ou sélection d'un son parmi un ensemble maximum de 8. Cette sélection est basée sur un choix préprogrammé de langues préférentielles.

D'autre part, le téléspectateur peut faire appel à des sous-titres s'ils existent, selon un choix préprogrammé de langues préférentielles. Le sous-titrage peut être également systématique pour les malentendants.

Outre le service TV, le terminal peut extraire d'un canal D2-MAC/paquets un programme radio. Il peut également accéder à un service de télétexte diffusé, avec les éventuels sous-titres, dans l'intervalle de suppression trame du signal D2-MAC/paquets.

Le terminal récupère aussi, quand il est présent, le service d'adressage sur antenne qui véhicule les messages relatifs à la gestion des titres d'accès.

2.2.2. Interface d'accès conditionnel

En plus de l'accès aux modes de consommation indiqués en introduction, l'interface d'accès conditionnel offre les fonctionnalités suivantes :

- Acquisition de droits gratuits pour la promotion d'un nouveau service ou à destination d'un nouvel abonné.

- l'occultation/sélection qui permet de restreindre les zones de réception de programmes par exclusion de certaines zones couvertes par la diffusion.

- l'empreinte digitale qui permet d'estampiller les programmes diffusés.

D'autre part, afin de faciliter la tâche du téléspectateur, lors de de ses dialogues liés au contrôle d'accès, une messagerie peut être introduite. son rôle est d'apporter soit des informations complémentaires, soit d'expliciter des informations codées.

Cette assistance au contrôle d'accès est diffusée sous forme de magazines de télétexte et constitue ce qu'on appelle le "télétexte d'assistance". Elle offre les prestations suivantes :

• Un téléspectateur peut vérifier le contenu de sa carte PC-Eurocrypt, de manière explicite.

• Un téléspectateur peut consulter les programmes à venir, avec les conditions d'accès qui y sont associées.

• Un téléspectateur n'ayant pas accès au programme en cours doit pouvoir en connaître le coût et les conditions d'accès jusqu'à sa fin.

2.3. Interface téléspectateur

On distingue trois types d'informations ou messages accessibles par l'utilisateur

2.3.1. Les messages à affichage automatique

• *Pour l'occultation et le remplacement* : en cas d'occultation, le signal reste embrouillé; une page de télétexte se substitue sur l'écran si celle-ci a été prévue par l'opérateur.

• *Messages d'introduction de la carte* : un message (carte absente, mauvaise introduction, carte défectueuse...) apparaît dans ce cas.

• *Informations sur programme en cours* : sur un programme non désembrouillé, présentation du contenu du programme.

• *Demande du code porteur* : le téléspectateur a la possibilité de dévérouiller certaines fonctions telles que la validation d'achat sur décision immédiate, le dépassement du niveau moral autorisé, l'accès à la zone de pré-sélection d'évènements, si l'accès à ces fonctions est protégé par l'introduction d'un code.

2.3.2. Les informations ou actions accessibles par intervention du téléspectateur

Informations sur le signal diffusé et les programmes :

A la demande du téléspectateur, le terminal présente :

• *Des informations sur le programme en cours* : une page d'information sur le programme fournie par l'opérateur est extraite du magazine de télétexte d'assistance, s'il est diffusé, ou à défaut de la voie "0" du D2-MAC/paquets.

• *Les informations sur les programmes à venir* : il est possible de consulter les programmes à venir sur une période de 7 jours, avec pré-programmation du réveil du terminal, en vue d'un enregistrement sur un magnétoscope et pré-achat (dans le cas d'une consommation différée).

• *Les informations d'identification de service* : afin de connaître le langues associées au programme TV et choisir l'une d'entre elles (outre le choix automatique des langues préférentielles effectué sans intervention du téléspectateur).

Configuration du terminal

Le téléspectateur peut intervenir sur :

• *La programmation de l'horloge du terminal* : en vue d'un réveil automatique du terminal.

• *La consultation de la carte* : elle permet la consultation des droits sur la carte, par opérateur et par type de service ouvert. Les titres peuvent être présentés de manière explicite si l'interprétation est rendue possible par la présence d'un télétexte d'assistance.

• *Les paramètres d'installation pour* :

- l'établissement d'une correspondance chaîne-fréquence, avec indication de la norme de diffusion utilisée (D2-MAC/paquets ou SECAM),
- le choix des langues préférentielles des sons et des sous-titres,
- la demande d'affichage systématique des sous-titres pour les malentendants,
- le choix du format selon le type d'écran de visualisation que possède le téléspectateur (soit 4/3, soit 16/9 ou biformat),
- le choix de la norme d'enregistrement (SECAM ou, à plus long terme, D2-MAC/paquets),
- la mise à l'heure de l'horloge interne du terminal,
- la sélection du plafond de niveau moral.

2.3.3. Accès à la messagerie individuelle ou collective

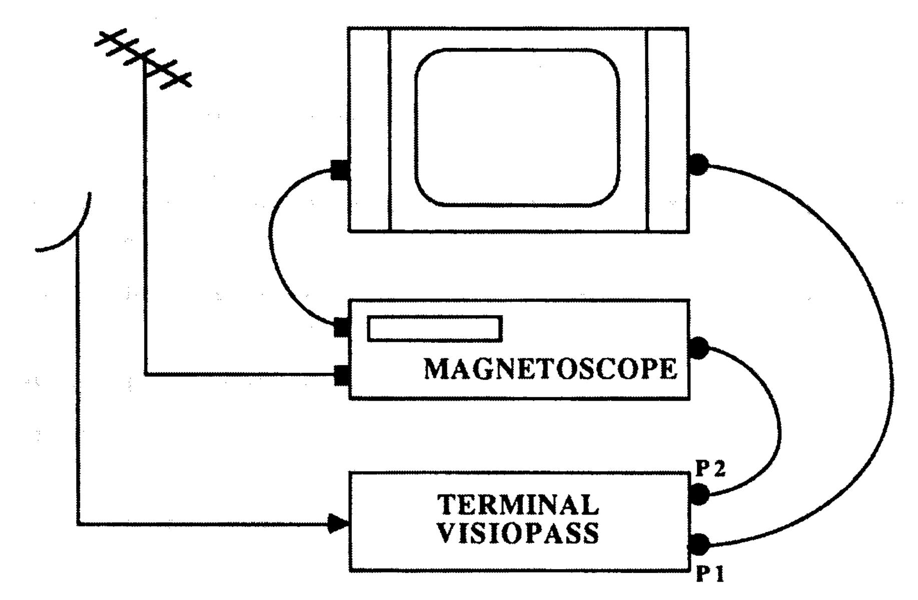
On distingue deux types de messagerie véhiculée par le signal D2-MAC/paquets :

• *La messagerie individuelle* : elle est diffusée, sous forme de page de télétexte, en association avec la messagerie de contrôle d'accès. Son arrivée est signalée au téléspectateur, par un voyant. Celui-ci y accède par pression sur une touche spécifique.Cette possibilité de messagerie individuelle est utilisée quand l'opérateur veut diffuser un message propre à un usager ou à un groupe d'usagers, voire à l'ensemble de son audience.

• *La messagerie collective* : En l'absence de message individuel, une page diffusée dans le télétexte d'assistance est affichée à la demande du téléspectaeur, en pressant la même touche que précédemment.

3. CONCLUSION

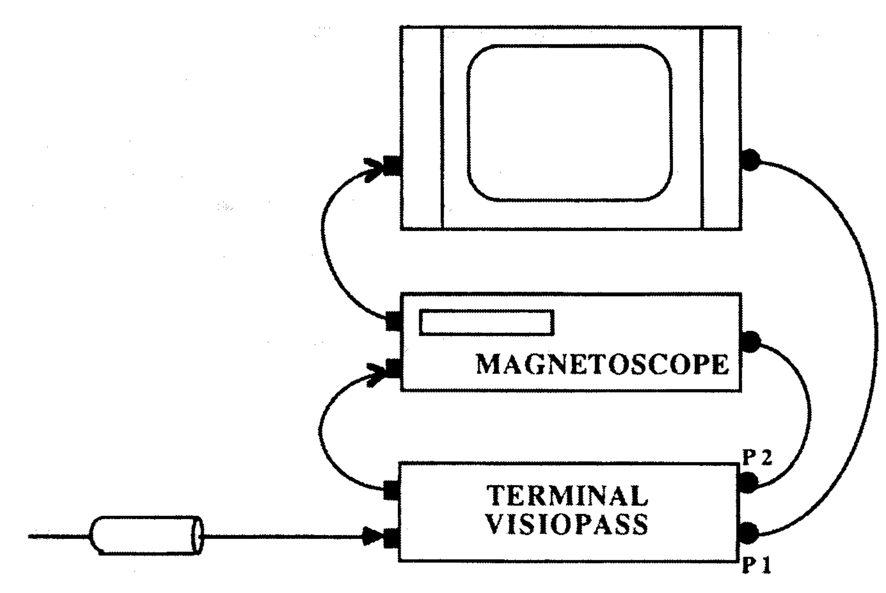
Cette communication a présenté une description fonctionnelle du terminal VISIOPASS, telle qu'elle est perçue par le téléspectateur, en soulignant les nouvelles possibilités ouvertes par l'utilisation du D2-MAC/paquets et d'Eurocrypt.



●: Prise Péritélévision

■ : Prise H. F.

Terminal VISIOPASS, version "satellite"



●: Prise Péritélévision

■ : Prise H. F.

Terminal VISIOPASS, version "câble"

FIGURE 1 : CONFIGURATIONS D'INTERCONNEXION DU TERMINAL VISIOPASS

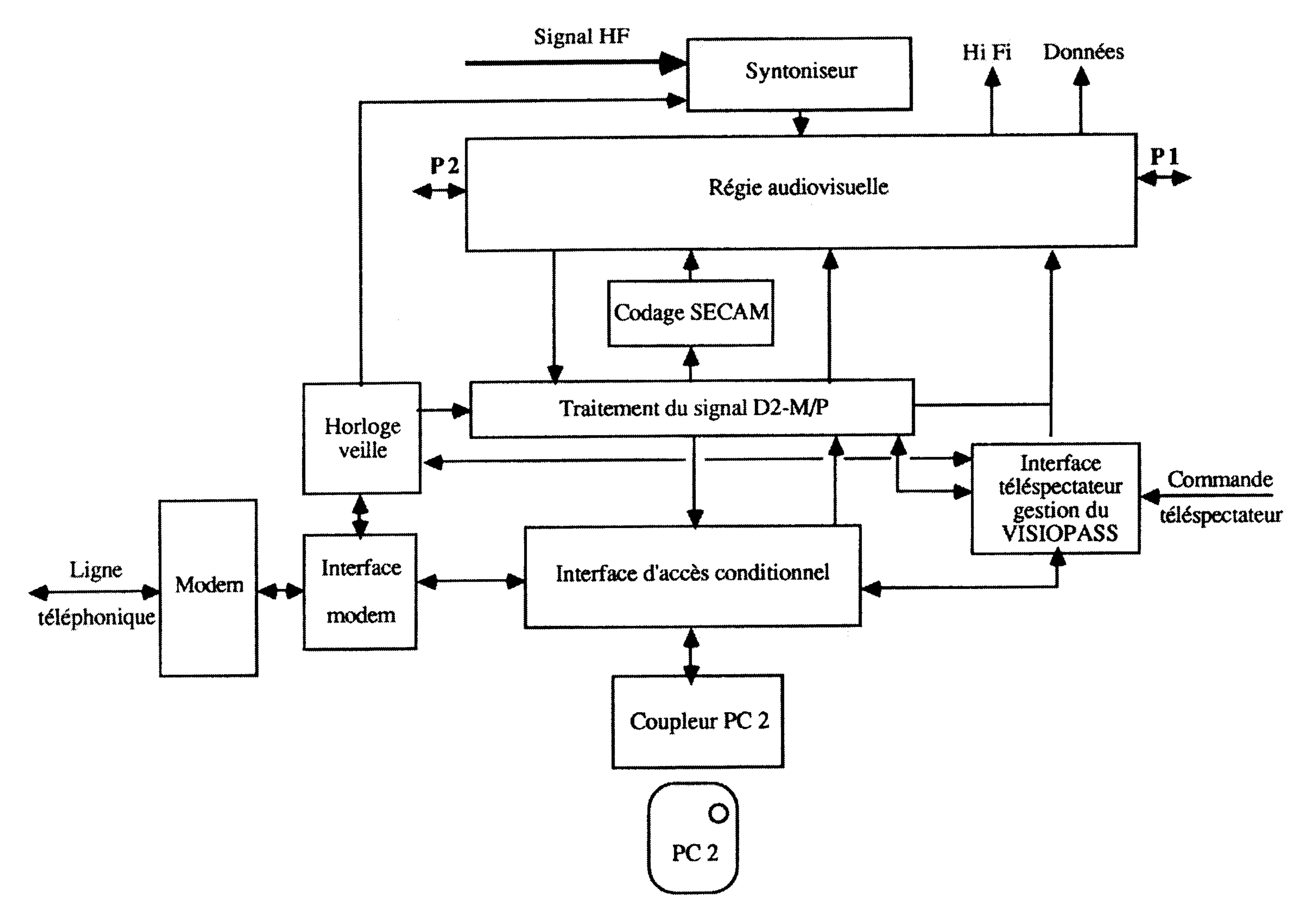


FIGURE 2 : DECOUPE FONCTIONNELLE DU TERMINAL VISIOPASS

CONDITIONAL ACCESS

AND THE USE OF D2B

Han **WELMER**
D2B Systems Co., Ltd
New Road
MITCHAM CR4 4XY
ROYAUME UNI
Tél : +44 81 685 12 12

ABSTRACT

With the introduction of Conditional Access, the consumer is confronted with a major problem : His Audio-visual system becomes much more difficult to control. Set makers and program providers also encounter problems, such as increased product complexity and diversity, and high investment costs. D2B offers solutions for the consumer in terms of ease of use and flexible system configuration. And it offers real benefits to set-makers, by separating independent product functions, eliminating repeated product development. Last but not least, D2B offers program providers an increased freedom of choice in CA-system.

TABLE OF CONTENTS

1. WELCOME

Good Afternoon ladies and gentlemen,

My name is Han Welmer. I work for the Company D2B Systems in London, and I am here to talk about the use of D2B in Conditional Access Systems.

2. SUBJECT OF THIS PRESENTATION

Since many of the earlier presentations held during this seminar, have discussed the system architecture of Conditional Access, I will not spend too much time on that subject. I will assume that you are familiar with it.

Instead I would like to concentrate on the relationship between Conditional Access and D2B.

To start with, I would like to explain what D2B is; what it is all about, and what you can do with it in the field of Consumer Electronic Products.

Next, I will focus on D2B and its relationship with Conditional Access. especially why should you use D2B in consumer products with Conditional Access? What are the benefits for the various involved groups: the users, the set-makers and the program providers?

Finally I will conclude with a short summary.

3. INTRODUCTION

3.1. What is D2B?

Let me begin by introducing D2B.

D2B stands for Domestic Digital Bus.

Based on advanced data communication technology, D2B makes it possible to transmit commands and related data between all kinds of consumer electronic products.

Of course, we have taken into account the generally applicable design rules, but we have also recognised the needs of CE products in particular, such as: Limited Cpu/Ram/Rom resources, real time requirements etc.

But D2B is more than just a data communication system. Because of its structure, it provides a framework for the compatible control of different products. Both between products of different brands, and between the products of today and tomorrow.

Within this scope, it is important to know that D2B has already been accepted as an standard by the IEC - the International Electrotechnical Commission.

3.2. Main purpose of D2B

The main purpose of D2B is to fulfil the needs of the consumer. We regard the wishes and requirements of the consumer as of paramount importance.

We believe that, above all, the consumer wants ease of use and convenient control of increasingly complex product functionality. With the introduction of the microprocessor and new media such as LaserDisc and Satellite Television, consumer

electronic products have become more and more complex to control. We recognise that a basic consumer need is to control this increasing complexity in a simple, convenient way.

But equally important, the consumer wants compatibility - both between brands and in the long term. He wants his current TV set to work with any peripheral, irrespective of the manufacturer and the time he buys it. And he even expects this to be true seven to ten years from now.

In order to achieve all this, and considering the fact that the C.E. business is a global business, it is obvious that international standardisation is essential.

But the typical procedure of international standardisation bodies such as the IEC is too slow for the fast-moving world of Consumer Electronics.

3.3. D2B Systems Co., Ltd. and its purpose

Therefore the neutral company 'D2B Systems Co., Ltd.' has been established.

This company has four major tasks. The first is to maintain the D2B standard and to develop new data protocols in order to allow new technological facilities to be incorporated.

A second role is to supervise those standards, in other words to ensure that suppliers and manufacturers stick to the rules governing compatibility.

A third task for D2B Systems is to support the industry with developments, information flow and interchange, so that all the participants can benefit. Of course, the absolute requirement for commercial security and confidentiality must be and will be met.

Finally, the need for harmonization with other existing and emerging standards has to be kept in mind.

4. D2B AND APPLICATIONS IN THE WORLD OF CONSUMER ELECTRONICS

4.1. Example: TV and VCR combination

But let's get back to the consumer, because that is after all the person for whom we all work.

The ultimate control system supporting 'ease of use' and 'control of complexity', provides the consumer with only two buttons: one to switch the system on and off, and another to select the desired facilities and services.

Let me explain this with a simple example involving a TV set and a Video Cassette Recorder. Assume you are watching an interesting programme and you wish to record it. To do this in today's situation, you have to first switch on the VCR, then find out which channel you are watching on your TV set, then tune the VCR to the same channel, and finally you can start recording.

4.2. TV and VCR combination with D2B

With D2B the procedure can be made much simpler - you just press the 'Record' button.

The rest can be done automatically: the VCR switches itself on, and using the resources of D2B it requests the channel to which the television is tuned. Next, it tunes itself to the same channel, and starts the recording. Remember, all you had to do was press a single button.

D2B even provides the tools for further improvement of the man/machine interface. For example, the VCR could send an On Screen Display message to the television via D2B, so that you get a clear indication of what is happening.

5. D2B AND CONDITIONAL ACCESS

5.1. Problem 1: increased control complexity

5.1.1. Introduction

And this brings me back to Conditional Access.

With the introduction of Conditional Access to the consumer, the complexity of the audio-video system is increased dramatically.

In the old days, when you wanted to watch a TV programme, you just selected the appropriate channel on your TV set.

Now, with Conditional Access, you have more products that need to be controlled. As well as your TV set, you need a satellite dish, a satellite tuner/decoder and a smart card.

5.1.2. Conditional Access and control without D2B

Without D2B, you have to control each product individually.

Specifically, if you want to watch a satellite program with conditional access, you have to take all the following steps:

1) switch on your TV set.
2) switch on the satellite tuner/decoder.
3) position the satellite dish.
4) select the correct channel on your TV, so that the signal from the satellite tuner is displayed.
5) select the right channel on your satellite tuner.
6) adjust any additional satellite reception parameters, whatever that might be.
7) insert the right smart card.
8) give authorisation to gain access.

Well, if consumers are just able to control a high end TV set and if many consumers have difficulty controlling a TV - VCR combination, do you think they will be able to control four products?

5.1.3. Conditional Access and control using D2B

With D2B, the user friendliness of the AV-System with Conditional Access can be improved dramatically.

All the user needs to find out is:

- which smartcard is needed for a specific program or channel and
- In which smartcard reader does this smartcard fit.

The rest of the control can be done via D2B. This is real user convenience.

5.2. Problem 2: dedicated products

5.2.1. Introduction

But there is a second field where D2B can improve the performance of an AV-System with Conditional Access.

As you all know, a typical satellite tuner/decoder is designed and produced for one dedicated service or Conditional Access System.

With Conditional Access applied to several programs, supplied by different broadcasters or Program Providers, the following problems arise.

For you as a consumer the problem will be that if you want to watch a program that uses a different Conditional Access System, you need a different tuner/decoder. Or if a broadcasting company decides to change to a new, more sophisticated Conditional Access System, you - as a consumer - will have to change your tuner/decoder as well.

Next to the big increase in the complexity of control, you will come up against a number of other problems. Such as interconnection problems, and how to find out - and remember - which smart card you need for which decoder.

5.2.2. Dedicated products and set-makers

For you as a set-maker, a dedicated tuner/decoder is also very unattractive, because a dedicated tuner/decoder is in fact a 'peaked' product - that is, it is targeted at a small market niche. This leads to complex version control, high production costs, high stock-keeping overheads and high distribution costs.

Secondly, building a decoder into a TV set or video cassette recorder may cause styling or mechanical problems.

A third problem, but certainly not the last one you will encounter, is the uncertainties regarding the specific Conditional Access System used by a broadcasting company. If this Conditional Access System is changed, a whole new design cycle has to be started for each individual product.

5.2.3. Why is it a problem?

So what causes all these problems with dedicated tuners/decoders to consumers and set-makers?

The reason is as simple as this: A decoder for Conditional Access, whether it is implemented as a stand-alone product or built into a TV set, video cassette recorder or any other product, really contains two functions:
- the basic signal processing and descrambling, and
- the Conditional Access Sub-System, or CASS, which grants access and controls the descrambling.

These two functions are generally defined independently. One example of a specification for the first function is the MAC family of television transmission systems.

But the MAC specification says little or nothing about Conditional Access. This situation led to the independent development of Conditional Access Systems such as Eurocrypt (as adopted by France Telecom) and Eurocypher (as adopted by BSB).

But the real controversy lies in the fact that these two functions are combined in a single product. And this will ultimately lead to problems and high costs for both set-makers and consumers.

5.2.4. Solution: one function in one product

To solve the previous problems, these two basic functions should be designed, developed and implemented separately.

This modular approach results in the development of single, independent, general-purpose functions.

For audio-video systems supporting Conditional Access, this results in two basic building blocks:
- a general-purpose receiver/decoder, which handles the signal processing, descrambling etc., and
- an external CASS, dedicated to a particular service or Conditional Access System. This building block handles the granting of access, storage of entitlements and control of the descrambling functions.

Each building block can be implemented in a variety of products.

If you want to be able to access three programs each having a different Conditional Access System, you only need one general purpose receiver/decoder. This unit can be implemented as a stand-alone D2MAC decoder or a set-top satellite tuner with a built-in decoder. It could even be built into a TV set or video cassette recorder.

Next you need three external CASSes, one for each specific Conditional Access System. They can all connect to the one and only receiver/decoder.

5.2.5. Benefits of separated functions

The benefits of this approach are obvious:

You as a consumer don't need many expensive receivers/decoders. In principle one general purpose receiver/decoder is enough.

You as a set-maker can focus on your specific product range. If you make TV sets or VCRs or satellite tuners, you don't want to be bothered with peaked products and details regarding decryption techniques and secure elements.

You as a broadcaster or program provider don't want to invest in expensive reception equipment to be installed at your audience. You want to optimise costs and revenues on transmission of programs and ensure that only your target audience can view your programs. Moreover, if you decide sometime in the future to use a more sophisticated Conditional Access System, you don't want to make a major reinvestment in the reception equipment at your viewers homes.

5.2.6. Requirements for the receiver/CASS interface

Of course, the general-purpose receiver or decoder and the external Conditional Access Sub-System will need to be interconnected.

As far as the consumer is concerned, any interface should be avoided, but if one is needed, it must meet the following requirements:

- The bus and the cabling must be easy to install by the consumer himself.
- The cabling must be flexible in topology. As far as possible, it must be up to the consumer to decide how to interconnect the various products.
- Of course, the interface must have a low cost, and various cable lengths must be available.
- And last but not least, the performance of the overall system must be excellent.

Of course, the set-makers have their own requirements, such as:

- The interface must be standardised and supported by the CE industry.
- The interface hardware must be cheap, reliable and available.
- It must be easy to make the interface comply with local rules and requirements, for example about aspects like safety, EMI compatibility and immunity to ESD.
- And - of course - the interface must be transparent in operation. Whatever the brand, performance or features set of the other product, the system must be sure to work in all circumstances.

6. BENEFITS OF USING D2B WITH CONDITIONAL ACCESS

All the above requirements AND ease of use AND long-term compatibility AND interbrand compatibility have been taken into account in the development of the D2B data protocols for Conditional Access.

Of course, anyone can compare D2B with any other standard or proprietary interface, in terms of its functionality as interface between a receiver and an external CASS. Such a comparison will show that D2B has the following benefits:

- D2B has been accepted as an international standard by the IEC
- D2B is supported by leading companies within the worldwide CE community
- D2B uses a low-cost, consumer-installable cable as the connecting medium
- D2B hardware such as ICs, sockets and cables are readily available from several suppliers
- Data protocols to implement Conditional Access are also available in the form of the D2B specifications
- D2B can also be used for other audio-video applications, which means that a single control bus can be used in the entire AV product cluster.

6.1. Long term benefits

By a series of evolutionary steps, D2B also meets another essential requirement: a flexible, long-term growth path.

For future products, for example, we can foresee developments like:

- Completely new descrambling techniques. In this case, only the decoders will have to be upgraded. The CASSes and smart cards can remain in use.
- Or alternatively, more sophisticated security elements may emerge. Again, no problem. In this case, only the relatively low-cost external CASSes will need to be replaced.
- Using D2B as a tool, a wide variety of man/machine interfaces can be built. This allows set-makers and broadcasting companies to distinguish themselves from their competitors.

- We can expect to see multi-CASS configurations, in which a consumer connects several CASSes to his single receiver/ decoder. This allows him to switch freely between different channels, carrying services using different Conditional Access Systems, all without the need to reconfigure his system or to switch smart cards.
- Along the same lines, one external CASS may be used by several receivers/decoders. This allows the consumer to change from watching a program on his TV set in the living room to watching it on the TV in his bedroom, without the need to take the smart card out of the first TV set and put in the second set.

7. SUMMARY.

To conclude, I would like briefly to summarize the main benefits that D2B has to offer:

- It is standardized, offering full inter-brand, inter-product compatibility, plus the flexibility to handle the extended feature sets of future products.

- It offers a real benefit to consumers, by simplifying and rationalizing the control of increasingly complex product functionality. Obviously, Conditional Access is an excellent example of a new and potentially very complex function for consumers to operate.

- And it offers real benefits to set-makers, by handling basic product functions in a standardized, transparent and economic way. In other words, the added value that D2B offers can be implemented at a low cost, without the need for repeated development effort for every new product.

- Finally, set-makers can call on D2B Systems Co. to provide them with support in the development and implementation of specific product functions through D2B.

I hope I have been able to give you some insight into the way D2B can play a part in increasing both the consumer-friendliness and the market-friendliness of Conditional Access.

Thank you very much for your attention.

BBC CONDITIONAL ACCESS TELEVISION SERVICES

S. R. ELY
BBC Research Department
Kingswood Warren
Tadworth
SURREY KT20 6NP
UNITED KINGDOM
Tél : +44 737 832361

ABSTRACT

During the past two years the BBC has gained experience with two subscription television services : one is the BBC TV Europe service which is relayed by satellite to cable and Direct-to-Home viewers outside the UK ; the other is a night-time downloading service on the BBC terrestrial UHF network. The search continues, however, for improved conditional access technology for these and other applications.

RÉSUMÉ

Depuis deux ans la BBC gagne de l'expérience en diffusant deux services de télévision à abonnement : l'un est le service "BBC TV Europe" diffusé en dehors du Royaume Uni par satellite aux réseaux câblés et aux foyers des téléspectateurs ; l'autre est un service de téléchargement utilisant pendant la nuit le réseau d'émetteurs terrestres de la BBC. Toutefois, on continue à rechercher la technique perfectionnée d'accès conditionnel pour ces applications-ci et pour d'autres applications.

TABLE OF CONTENTS

1. INTRODUCTION

The BBC is active in the subscription television market and is encouraged by the UK Government to develop subscription services as a way of supplementing its income from the licence fee [1]. Indeed, the BBC has been working in the field of Conditional Access (CA) Television for many years. Initially this work was directed towards CA systems applicable to Direct Broadcasting by Satellite (DBS) [2] and BBC Research Department assisted in the development of the CA systems specified for the EBU MAC/packet family of systems.

Recent BBC work on CA television systems has been primarily directed towards the application of CA techniques to night-time downloading services broadcast via the existing BBC UHF terrestrial television network [3]. In this application, the network of terrestrial transmitters is used outside normal programme hours to broadcast, in scrambled form, signals to be recorded, via a descrambler, on domestic Video Cassette Recorders (VCRs) ready to be replayed at a time convenient to the viewer.

Since June 1987 BBC Enterprises Ltd (a wholly owned commercial subsidiary of the public service BBC) has, as part of its television programme export business, distributed BBC television programmes in scrambled form via Intelsat V to cable systems in Scandinavia and elsewhere. Since April 1989 this BBC TV Europe service has been extended to include Direct-To-Home (DTH) subscribers.

BBC Enterprises also plan to start a new CA service to be relayed via one of the transponders of the Olympus experimental satellite later this year.

These three ventures will enable the BBC to gain hands-on experience with a range of subscription services. However, because of a wish to develop these new services as quickly as possible, it has been necessary to adopt and adapt existing CA technology rather than specify purpose-designed systems and equipment.

The purpose of this paper is to outline the requirements and constraints which must be met by CA techniques applied to these services, and report the results of laboratory and over-air tests aimed towards finding suitable CA systems. We will concentrate mainly upon the terrestrial downloading service which offers the greatest technical challenges.

2. REQUIREMENTS TO BE MET

In any conditional access television system there are, of course, essentially two distinct elements:

i) Scrambling: i.e. the processes whereby the picture and/or the sound signals are rendered unusable without an authorised descrambler.

ii) Access control: i.e. the processes whereby information is provided to enable authorised viewers to descramble the service. The availability of this information is controlled by transmitting it in encrypted form. The scrambling is closely associated with the signal coding and the transmission systems and media. The access control systems are more closely aligned with the business systems and the interface with the customers.

The requirements to be met by the scrambling and access control systems may be considered in terms of the following headings:

2.1 Opacity

The degree to which signals are disguised in scrambled form is termed opacity. Whilst some applications need the scrambled signals to be totally unrecognisable, in other cases less opacity may be advantageous so that the viewers can be tantalised to subscribe to the service.

2.2 Transparency

The quality of the picture and sound signals after the scrambling and descrambling processes indicates the transparency of the scrambling systems. Ideally, of course, the processes of scrambling and descrambling should produce imperceptible degradation to the signals. It is especially important to note that distortions inherent in the broadcast chain, propagation effects, or receivers can degrade transparency.

Another major form of impairment to a CA service is unreliable acquisition of the access control data. It is therefore important that the over-air data required for the distribution of access control signals can be reliably received even under adverse reception conditions. For example, access control data should be reliably receivable at signal-to-noise ratios below those needed for usable picture and sound signals. Furthermore, any auxiliary system used for distributing access control information, such as postal distribution of smart cards, or telephone answering services needed to facilitate over-air authorization must also be reliable and convenient to use.

2.3 Security

Security depends upon all elements in the system including the scrambling and access control systems, key distribution, encryption of over-air access control data, security of subscriber management computer systems, and security in the factories producing the decoder and/or the access control module: security is limited by the weakest link in this chain.

No CA television system can be guaranteed to be completely secure particularly bearing in mind the relatively long lifetime during which the system is expected to resist attack. For most CA services it is sufficient to make piracy uneconomic rather than impossible. A particular security risk occurs, however, when service is not legitimately available in a country where it is technically possible to receive the signals. In these circumstances customers for pirate decoders may be willing to pay more than the cost of the legitimate access in order to receive the service.

2.4 Cost

The cost of the CA decoders is usually a major factor in the economics of a subscription service. Unless existing decoders provided for other CA services can be used then all legitimate customers must first be equipped with a CA decoder before they can access the programmes.

If customers must pay for their decoders directly, then this initial outlay will form a barrier to the take-up of the service. Alternatively, if the broadcaster pays the capital cost of the decoders and then hires them to his customers, the capital cost plus interest has to be recovered as part of the subscription. This amortisation element in the subscription may well be a major part, thus leaving little funding to pay for good programmes.

A further cost consideration is that of the capital and revenue cost to the broadcaster of setting up and running the transmitting end of the CA broadcast system. This capital cost includes that of the scrambling and encryption equipment and the computer systems and software needed for the subscriber management system. These capital costs may be large if significant hardware or software development is needed.

Another potentially major element in the revenue cost of a CA service is that of running the subscriber management system, including invoicing, and processing payments by customers. Some economies of scale may be realised here by using agency services who operate such customer management services for other broadcasters or, indeed, other businesses.

2.5 Compatibility

2.5.1 Compatibility with existing receivers

Unlike enhancements such as teletext or stereo sound, which are intended as compatible enhancements to existing broadcasts, CA services are not, by definition, compatible with existing receivers since all viewers will need a decoder (or, in the longer term, a new receiver with an integrated decoder). However, it is important to be able to interconnect the decoders easily with existing receivers and VCRs. This interconnection must not interfere with reception of other services or reduce the facilities for recording and replaying other services via the VCR.

In France and some other European countries this interconnection problem has been greatly reduced by the mandatory provision of a SCART (peritelevision) connector on all television receivers and VCRs. This SCART socket provides baseband video input and output which can be routed as required via the CA decoder. Unfortunately, in the UK, SCART sockets are not mandatory and only a minority of receivers are equipped with baseband video input. Thus the only universally available input to existing UK receivers is the aerial socket. Whilst this presents few problems when just one device (e.g. a VCR) is connected in this way, it is very much less easy to install several devices (e.g. satellite receiver(s), CA decoder(s), and VCR(s)) in this way and tune the local remodulators (which are full double-sideband) so as to avoid mutual interference or interference with off-air signals. Also, of course, such an r.f. composite PAL interconnection does not allow the viewer to benefit from the potentially better quality pictures available via MAC services.

2.5.2 Compatibility with other broadcast services

CA signals must not cause interference to other broadcasts sharing the same or adjacent channels. Therefore existing planning limits for Co-Channel Interference (CCI) and Adjacent Channel Interference (ACI) must not be exceeded. Conversely, the scrambled signals should not be more susceptible to these interferences than clear signals. In practice, it is usually found that scrambling the picture and sound signals actually reduces the effects of CCI and ACI both from and to the CA signal.

2.5.3 Compatibility with existing distribution and transmitter networks

Where, as in the case of the BBC night-time downloading service, a broadcaster seeks to transmit programmes via an existing network which was not designed with CA in mind, there is the added complication of making the CA system compatible with the existing broadcast system and equipment or vice-versa. This is a particular constraint where, as in the BBC's case, it is required to broadcast conventional clear PAL signals during one part of the day and CA programmes during another.

The scale of a terrestrial broadcasting network such as that operated by the BBC, which comprises transmitters at nearly one thousand sites and the associated point-to-point distribution system, militates against almost any changes to the network to accommodate CA signals. Furthermore, unlike a cable system or a satellite transponder, a terrestrial broadcasting network is not transparent to the signal it conveys. The following factors must be taken into account:

i) Non-uniform amplitude-frequency response due to instrumental imperfections (e.g. filtering) in practical Vestigial SideBand Amplitude Modulation (VSB-AM) transmission systems. This is a major difference from satellite systems which are conveyed using Frequency Modulation (FM). Aberrations in the amplitude-frequency response of the path used to convey the scrambled picture signal seriously impairs the quality of the descrambled pictures in many systems.

ii) Distortions due to transmitter non-linearity (including differential gain and differential phase effects). This is a significant difference between cable systems (which also use VSB-AM) and terrestrial broadcasting networks.

iii) Restrictions on the video signal voltage envelope: terrestrial transmitters cannot be considered as simple linear amplifiers but are carefully optimised to radiate the standard PAL or SECAM waveform. Neither the luminance nor the colour components may extend beyond their normal video amplitude ranges.

iv) Need for standard signals in the horizontal and vertical blanking intervals. All the available lines in the vertical blanking interval of existing BBC terrestrial broadcasts are allocated to teletext or test-waveforms. The waveform in the horizontal blanking interval is used for automatic gain control and clamping.

v) Many modern high-power transmitters include energy-saving systems such as klystron pulsing, which changes the picture-to-sync timing slightly.

vi) Interaction with digital signal processing in distribution networks:

a) Present-day use of Sound-in-Syncs (SIS) for distribution of sound signals: for many years the BBC and other broadcasters have used SIS to distribute sound signals to main transmitters. At the transmitters the SIS signals are decoded and conventional syncs restored for transmission. Therefore, it is not feasible to distribute scrambled signals which modify the horizontal syncs since these could not be conveyed via the existing distribution network and scrambling at every main transmitter would be expensive. The SIS equipment introduces significant and, in some cases variable, differential delay between sound and vision. Account of this must be taken if the sound and picture scrambling systems use related timing signals.

b) Future Digital Distribution Networks: in the near future the BBC and many other broadcasters expect to use digital signal distribution systems for both picture and sound signals. Such systems will almost certainly use bit-rate reduction techniques and these are incompatible with nearly all scrambling processes. This is because scrambled signals do not have the redundancy which bit-rate reduction systems exploit. It must therefore be accepted that the only way to distribute CA signals via such digital systems will be to descramble before bit-rate reduction at the sending end and re-scramble at the far end of the link. It is, however, expected that, since the signals are already in digital form at these end-points, the additional cost of these CA processes will be relatively small. This is especially so if the need for this is foreseen before the digital distribution network is installed.

2.6 Flexibility

Flexibility is usually an important requirement for the access control system. The broadcaster and his customers may want the possibility of many different access modes including provision of multiple tiers, multiple logical channels on the same physical channel, regional blackout, pay-per-view, impulse pay-per view etc. In particular, there is a strong advantage in being able to evolve from a simple system at the start of service to a more sophisticated one, including the option of changing or modifying the security device, to combat piracy.

2.7 Standardisation

It can be argued that, in order to allow a free market for subscription television programmes to develop, the interests of the viewers would best be served by standardisation of CA systems such that customers need only one decoder to access all the available services. Furthermore, such standardisation would provide economies of scale in manufacturing and simplify maintenance.

So far, however, many operators of European CA services have chosen to use proprietary CA systems which do not give their customers access to competing CA services. It remains to be seen, however, whether the expected customer resistance to buying and installing multiple decoder boxes will force standardisation and what strategic alliances emerge, especially amongst the smaller operators who cannot afford the development costs of an exclusive system.

2.8 Man-machine interface

The importance of simple and reliable operating controls for the CA receiver/decoder must not be under-estimated. To access services funded by licence fee or by advertising the customer has to do little more than turn his receiver on and switch to the desired channel. Subscription services therefore face an immediate handicap if the customer has to follow a complicated or tedious procedure to gain access: even relatively simple tasks become tiresome if they have to be repeated frequently, and UK audience research studies indicate the majority of UK viewers are unable or unwilling to follow complicated procedures such as that needed to set-up a VCR for time-shift recording.

This is especially relevant for a night-time downloading service: successful access to downloading services requires that a VCR be set-up to record the desired programmes. The use of the normal VCR time-shift recording functions is not satisfactory, mainly because, as indicated above, this is too difficult or too tedious for the viewers to use regularly. Furthermore, it is very desirable in such a night-time service for the broadcaster to retain flexibility to change the schedule e.g. to accommodate a delay in the start of the night-time schedule due to an extra programme earlier in the evening. Indeed, in some circumstances the broadcaster may need to switch a particular programme from one network to another at short notice. Thus some means of automating the VCR recording function is essential for a downloading service.

3. BBC OPERATIONAL EXPERIENCE WITH CA SYSTEMS

3.1 The BBC TV Europe service

The BBC TV Europe service delivers, via the East Spot beam of the Intelsat V (27.5° W) satellite, BBC television programmes to about half a million viewers, most of whom are in Scandinavia and receive their signals via cable systems. In such cases, the descrambler/decoder is at the cable-head and the viewer receives clear signals. However, since April 1989, BBC TV Europe decoders have also been available for Direct-To-Home (DTH) reception. About 3000 authorised BBC TV Europe DTH decoders are in use.

(N.B. As a well-established and separate venture, BBC-1 (and in some cases BBC-2 as well) programmes are distributed from the UK by terrestrial microwave link to cable systems in parts of Belgium, France and the Netherlands. The signals of this terrestrial distribution system are not scrambled).

The scrambling system used on the BBC TV Europe service is the SAVE system, manufactured by Sat-Tel Ltd.

The picture scrambling comprises inversion of the complete video waveform, the addition of a "spoiling-tone" at about six-times line-frequency, and the addition of pre-emphasis.

The sound scrambling originally comprised spectral inversion of the analogue sound signal. (In this commonly used method of sound scrambling the spectrum of the baseband audio signals is reversed by selection of the lower sideband after suppressed carrier amplitude modulation of a subcarrier in the region of 12 to 16 kHz). Since early 1989,

however, the sound scrambling has been changed to be a variable frequency-shift rather than spectral inversion. A wide-range of frequency-shifts can be accommodated and decoded and this new sound scrambling is claimed to be more secure than spectral inversion.

The SAVE system does not use over-air access control signals and therefore the "key" mainly comprises possession of a decoder. The decoders, however, have a user replaceable external "dongle" which programs certain parameters of the descrambling algorithms. The dongles may be changed to combat piracy.

DTH viewers pay for the service by a period subscription, which is included in the initial cost of the decoder. This grants access up to April 1991, after which the CA system is expected to change.

The SAVE system is relatively insecure and significant piracy has occurred in the past. However, the recent improvements to the system, together with legal action in the UK against suppliers of unauthorised decoders may reduce this problem.

The picture descrambling system is sensitive to non-linear distortion: the latter produces harmonics of the spoiling tone which cannot be removed in the decoder. The main cause of non-linearity in the FM satellite system is the receiver. Professional receivers used at the head-end of cable systems produce few problems in this respect, but the use of customers' existing satellite receivers for DTH reception has given rather more variable results.

The choice of CA system to be used by BBC TV Europe after April 1991 is still under consideration and may well be influenced both by the choice made for the terrestrial PAL downloading service and by the results obtained with BBC Enterprises' proposed service on the Olympus experimental satellite.

3.2 The Night-Time Downloading service

In February 1988, the BBC received UK Government approval for a two-year period of experimental night-time downloading broadcasts in association with British Medical Television (BMTV). This service broadcast medical news and educational programmes produced by BMTV. It was necessary to scramble the picture and sound signals mainly for reasons of medical ethics.

In January 1990, after several months of regular broadcasts to around 4000 decoders, BMTV ran into financial difficulties, and the service was suspended. Although the future of BMTV is uncertain, the BBC is keen to develop the downloading service and has set-up a new division of BBC Enterprises Ltd (BBC Subscription Ltd) to expand the service on a broader base of programming and with new CA technology (see below).

Valuable experience was gained with the BMTV service. The basic CA technology used was adapted from the Philips (RPIC) Discret-1 system which is well established (in its SECAM-L form) on the Canal Plus network in France and (in PAL B/G form) in Switzerland. In both these major applications, and in many other smaller scale applications throughout Europe, the Discret-1 system has proved very successful.

The picture scrambling of the Discret-1 system comprises moving the active-line period of the video waveform a few microseconds relative to syncs on a line-by-line basis. This system is relatively immune to the distortions inherent in the terrestrial broadcast chain, and is compatible with existing analogue video distribution systems and transmitters. Although the scrambled picture signal is not particularly opaque, and the system is not very secure, neither of these limitations proved significant in the BMTV service.

The sound scrambling of the Discret-1 system is, in common with the original SAVE system, spectral inversion of the analogue sound signal. There is some loss of quality in the descrambled sound signal due to reduced bandwidth and decreased signal-to-noise ratio. Increased buzz-on-sound was perhaps the most noticeable impairment but this was not found to be a significant problem in the BMTV service.

The standard Discret decoders had to be modified for the BMTV downloading service to include the following features:

1. UHF interconnection to the VCR and receiver (normally this is a baseband connection via the SCART).

2. Automatic VCR control via an externally connected programmable "universal" infra-red remote controller.

Both of these additional features made it significantly more difficult for the end-user to install and set-up the decoder. These installation problems were exacerbated by the signals of CA service being on-air only during the brief night-time programmes. This made it difficult for the customer to confirm that the equipment had been correctly installed and set-up. Furthermore, it was difficult to identify what had gone wrong if a VCR failed to record the downloaded programmes correctly.

Solving these installation problems is, therefore, amongst the highest technical priorities in developing the downloading service. It is also desirable to use more sophisticated CA systems which will offer better security, opacity and flexibility. The search therefore continues for a second generation CA system suitable for use in the downloading application on the BBC UHF terrestrial PAL network.

3.3 BBC Enterprises' service on the Olympus Satellite

The BBC Enterprises service on the Olympus satellite (European beam DBS channel 20) is not yet fully operational, and the choice of CA system has yet to be finalised. The availability of suitable receiver/decoders for the target audiences is expected to be a prime factor in this choice. At present the BBC TV Europe service is carried (in clear D2-MAC) during the evenings. During the day this channel carries the EuroSTEP educational project.

4. THE SEARCH FOR A SECOND GENERATION CA SYSTEM FOR THE BBC TERRESTRIAL DOWNLOADING SERVICE

4.1 Picture scrambling systems

For terrestrial PAL based services the most promising contenders for a secure picture scrambling system are Active Line Rotation (ALR) and Line Shuffling. Until recently, BBC work has concentrated on ALR scrambling because of the relatively large amount of memory required for line-shuffling over sufficient lines to give adequate security and opacity.

4.1.1 Active Line Rotation

Active Line Rotation (ALR) scrambling of PAL signals is closely related to the component rotation scrambling method used in the MAC/packet system [4]. As is well known, ALR scrambling comprises cutting and rotating the active-line video information so that the segments on either side of the cut-point are interchanged. In some implementations the order of the samples in one of the segments is also time-reversed. It is not, however, clear that this modification gives any advantages and it is more difficult to implement.

ALR PAL scrambling is now, of course, becoming well established as part of the Videocrypt CA system which is used on some of the Sky broadcasts via the Astra satellite. However, for VSB-AM terrestrial PAL broadcasting there has always been concern that ALR scrambling is susceptible to line-tilt.

Line-tilt can occur due to a large variety of causes in VSB-AM transmission. For clear pictures the small resultant change in luminance from one side of the picture to the other is not perceptible for moderate amounts of tilt. However, if tilt occurs anywhere in the transmission of an ALR scrambled signal then the descrambled picture has, in effect, a low-level scrambling pattern superimposed on it. This appears as "streaky" noise.

Informal subjective tests on critical pictures (notably ones with plain backgrounds at moderate luminance levels) indicated that streaky noise becomes perceptible on the descrambled ALR picture when the line-tilt exceeds about 0.5%. (Line-tilt is defined here as the difference in amplitude between the ends of the scrambled active-line expressed as a percentage of the black-to-white excursion of the wanted luminance signal (nominally 0.7 volts)). This accords well with the results obtained for double-cut component rotation of MAC signals [4]. These and other results suggest that for the downloading service (in which the descrambled pictures are viewed after recording and replay by a domestic VCR) the maximum tolerance for line-tilt due to all contributions up to and including the descrambler should be around 1.5%.

In BBC laboratory tests to investigate the causes of line-tilt in VSB-AM receivers, it was found that inaccuracy in the vestigial sideband frequency response of the receiver is unlikely to be a major source of line-tilt. This is because, unless the vestigial sideband filter is very irregular at frequencies very close to the i.f. vision carrier frequency, the i.f. response cannot cause significant amplitude response aberrations in the very narrow band of video frequencies (less than 30kHz) which are critical for line-tilt. Thus it was concluded that VSB-AM tuners for use with ALR scrambling do not need special i.f. filters or very accurate automatic frequency control.

It was, however, found that automatic gain control (a.g.c.) circuits are very critical in determining tilt performance: small amounts of picture- dependent ripple on the agc line were found to cause significant multiplicative distortion which manifests itself as line-tilt.

In December 1988 the BBC carried out extensive out-of-hours field-tests of ALR scrambling on its terrestrial UHF network. It was found that, of those tested, all the main stations gave acceptable (in the context of the downloading service) descrambled pictures. The measured tilt was in all cases less than 1.5% and the impairment due to scrambling less than one grade on the CCIR 5-point quality scale (results from informal subjective tests).

From the relay stations the results were more variable: in the case of the notorious chain of five relay stations in tandem from the Wenvoe main station, it was found that the tilt was not cumulative along the chain and was worst at Brecon (number three in the chain of five) where about 3% tilt was measured.

In most cases it was found that there were two components to the tilt: a line repetitive element (i.e. as if a constant amplitude luminance saw-tooth were added to the picture-signal) and a picture-dependent element. In most cases the line repetitive component of tilt was found to be such that the amplitude of the luminance signal decreased along the length of the active line. This is as would be expected if the cause were poor l.f. video response. However, in a significant number of other cases the tilt was in the other direction, as if the video response were boosted at low frequencies.

In some cases the tilt varied significantly over a time period of a few seconds. This was apparently correlated with movements of the receiving aerial (which was mounted on a 10-metre mast on the survey vehicle) in the wind. This suggests that propagation effects such as multipath also contribute to tilt.

It was also found that under some conditions of multipath propagation the cut-points on each line became visible as white or black dots (like flies) on the descrambled picture. It is believed that this effect could be reduced by providing a greater overlap at the cut-points, although this would be at the expense of a further slight decrease in the width of the descrambled picture (thus giving a narrow black border down the sides).

Further investigations have suggested that there are many different causes of tilt in the network. It is believed that one common cause may be picture-dependent ripple in the a.g.c. circuits of transmitters and re-broadcast relay receivers.

The line repetitive component of tilt could relatively easily be removed by a simple compensation circuit in the decoders using a test-line in or near the vertical blanking to determine the correction necessary. The picture-dependent tilt would be more difficult to correct in the decoder though it has been suggested that this might be attempted by measuring the difference in the amplitudes of the ends of the scrambled line. The time-dependent tilt could be removed providing that the correction circuits can respond quickly enough.

It would, of course, be preferable to eliminate tilt from the transmission system rather than correct it in the decoder. However, given that tilt due to propagation effects cannot be thus removed, improvements to the transmission network would not completely eliminate the problem of tilt. Furthermore, it seems unlikely to be economically feasible to reduce tilt to the required tolerance throughout the existing BBC network, particularly since it was found that the tilt introduced by transmitter stations changed significantly between two sets of measurements a few months apart.

Thus it is concluded that ALR scrambling could be used for the downloading service providing that it is accepted that either:

Some viewers, especially those who watch via a relay station (less than 10% are thus served), will see perceptible streaky noise on their descrambled pictures.

or

Decoders should include tilt-correction (yet to be designed and proved effective).

4.1.2 Line-shuffling

There is much less information yet available about the suitability of line-shuffling picture scrambling systems. However, providing the shuffling interval is sufficiently large, the opacity can be similar to that of ALR scrambling and it avoids the problems of line-tilt. Field-tilt could, however, be troublesome unless very effective clamping is provided. Moreover, for PAL signals (with SECAM this problem does not occur) there may be a problem in making line-shuffling secure: this is because if the colour-burst is shuffled with the associated active-line then the phase of the burst gives a strong clue as to where the line belongs in the descrambled frame. Alternatively, if the burst is not moved with the associated active-line, then timing-jitter and propagation delay fluctuations could be troublesome.

The BBC is currently investigating line-shuffling scrambling systems as a possible alternative to ALR for the downloading service.

4.2 Sound scrambling systems

4.2.1 Analogue FM sound

The most commonly used method of scrambling sound signals for broadcast via the analogue FM channel is the spectral inversion method outlined above. Although insecure, it is moderately opaque and provided care is taken in implementing the system (especially the filtering) moderately good quality sound signals can be delivered.

There are few viable alternatives to spectral inversion if analogue transmission is to be used. Frequency shifting, as in the present BBC TV Europe system, may offer slightly better security but is less opaque.

Another approach involves dividing the analogue sound signal into segments in the time domain and then transmitting the segments in a random order or time reversing each segment, or both. This method offers moderate opacity for speech signals although music is poorly disguised. Using a large number of segment permutations the system could be made secure.

One major problem with this method, however, is the need to provide markers to identify the boundaries of the segments in the decoder. The vision signal cannot be used for this purpose because in a complex terrestrial distribution network there is variable time delay between the paths taken by the vision and sound signals. In a BBC experimental system a low-level pseudo-random binary sequence, conveyed at very low level in the analogue audio channel itself, and recovered by correlation in the decoder, was used with some success. However, the system was impaired by distortions in transmission and causes large delays in the sound signal path (and therefore needs compensatingly large delays in the vision signal path). This system has, therefore not been developed further.

4.2.2 NICAM 728 digital sound

The NICAM 728 digital sound system, which was developed by the BBC for use with its terrestrial PAL broadcasts [5], could relatively easily be adapted to convey the digitised sound signals in scrambled form. This would, of course, provide a secure and transparent system capable of conveying two high-quality sound signals. Indeed NICAM 728 signals are already scrambled for energy dispersal purposes and it would be a relatively simple matter to replace the simple linear-feedback pseudo-random binary sequence (prbs) generator used for this purpose by a secure CA sequence generator. This could be similar to those specified to scramble the sound signals in the MAC/packet system.

However, at present only one main BBC transmitter (at Crystal Palace in London) is yet equipped for NICAM broadcasts, and even by the autumn of 1991, when the BBC plans to start a NICAM 728 service, only ten of the main stations (covering about 74% of the population) will be equipped for NICAM. Therefore NICAM 728 cannot, in the near future, be used on its own to convey scrambled sound signals for the downloading service.

Nevertheless, BBC Research Department is developing an experimental CA NICAM system. This might be used on the downloading service to provide better quality and stereo sound where NICAM reception is available. It might also be used on the BBC TV Europe satellite service if that continues to use PAL after April 1991.

4.3 Access control systems

Access control systems and the associated encryption of the over-air data are in principle independent of the coding used for the picture and sound signals or the medium used to convey them. Accordingly, it would seem feasible to adopt for BBC use the security module, subscriber management systems etc. used in any other CA system, independently of whether it was designed for MAC/packet, PAL or SECAM services.

This could provide the flexible and secure access control system which the BBC, in common with most other operators of CA services, expects to need. By adopting an existing access control system there would be obvious economies of scale in the production of equipment and software, and the possibility of synergistic sharing of subscriber management systems.

However, one significant difference between PAL broadcasts and MAC/packet services in this context is that PAL broadcasts do not inherently provide a means of conveying the data-signals needed by CA systems. There are, however, a variety of proven methods for adding data signals to PAL broadcasts.

The Discret-1 system conveys the data needed to synchronise the decoders and to provide tiering information using a low-rate data-signal conveyed in a line at the bottom of each active field. This is reblanked in the decoder and so the data is not visible on the descrambled picture. Whilst such a low-rate data system is highly reliable, it cannot provide the data capacity needed for an over-air addressed system, if that option is needed. For over-air addressing in a terrestrial PAL service, teletext conveyed in the vertical blanking seems to be the only viable system.

The suitability of teletext to convey CA data has been studied in a number of over-air tests. These tests were somewhat inconclusive: it was found that using a professional quality teletext receiver/decoder adequately reliable teletext reception was possible at all reception sites within the service area. However, it was also found that teletext reception is significantly more fragile, especially under conditions of multipath propagation, than the other elements of the CA systems tested.

These tests could not, however, establish, what proportion of viewers could receive teletext adequately reliably using their existing aerials. This factor could be important in the development of a downloading service since the cost of checking and improving aerial systems might significantly affect the economics of the service.

There are, of course, possible ways of improving the ruggedness of teletext reception using echo-cancellers and/or enhanced error protection on the CA data. These possibilities are under study.

4.4 Programme delivery control system

As mentioned above, automation of the VCR recording functions under the control of the broadcaster via over-air signals is regarded as essential for the development of night-time downloading services.

In the BMTV downloading service automatic initiation of recording was achieved by triggering the VCR to record whenever the Discret decoder detected the presence of a Discret signal which it was authorised to receive. When the Discret signal was removed from the network at the end of the downloading programme, or changed to another tier, the decoder ceased to be authorised and thus after a short-delay, the VCR was stopped and put into standby.

No special over-air data for VCR control (other than the standard Discret control signals in line 310 of each frame) was required. Although this simple system was adequate for the BMTV application, a more flexible programme delivery control system, allowing, for example, the decoder to be switched to another channel, is desirable.

There are many commonalities here with the proposed Programme Delivery Control (PDC) systems which are under study in the EBU [6]. The use of a PDC system seems to offer the best way of controlling the VCR for downloading CA programmes. In the short-term, however, existing VCRs will not have PDC functions built into them. Therefore, if it is necessary to use the customers' existing VCRs for the downloading service, the preferred solution seems to be to build a PDC decoder into the CA decoder and use it to operate the VCR via a "universal" infra-red controller.

5. CONCLUSIONS

The choice of CA systems for use in the BBC's two initial ventures into subscription television (the BBC TV Europe service and the BMTV night-time downloading service to doctors) was limited by the need for assured availability of equipment for an imminent start of service and a proven track-record of the basic CA technologies used. With these constraints, the systems chosen were inevitably relatively simple first generation CA systems which did not entirely meet all the ideal requirements. Nevertheless, valuable experience has been gained with these systems, and they have pointed the way towards more sophisticated systems which can fulfil the needs of longer term developments of these services.

The BBC remains keen to develop the market for subscription television. A new team in the recently formed BBC Subscription Ltd is urgently studying the choice of CA system for use in the terrestrial night-time downloading service which they plan to re-launch with new technology and broader based programming early in 1991. In the meantime, the BBC TV Europe service on Intelsat V continues and a new BBC Enterprises service on the Olympus experimental satellite is planned to start later this year.

6. ACKNOWLEDGEMENTS

The author is grateful to the Director of Engineering of the BBC for permission to publish this paper and also wishes to acknowledge the contributions to this work by his colleagues at BBC Research Department, and at BBC Enterprises Ltd.

UN MODULE DE SÉCURITE DÉTACHABLE

POUR LA TÉLÉVISION À PÉAGE

Pascal **BENOIST**
Bull CP8
1 rue Eugène Henaff
BP 45
78193 TRAPPES
FRANCE
Tél : +33 (1)30 69 54 01

RÉSUMÉ

La mise en œuvre d'un système de télévision à péage oblige à trouver des solutions aux problèmes induits par le mode de paiement souhaité.
Pour remplir sa mission, un tel système doit être gérable, efficient, fiable et sécuritaire.
Pour atteindre ces objectifs, la solution retenue est basée sur l'utilisation d'un module de sécurité détachable, la carte PC2.
Ce module enregistre les droits d'accès au programme et sert de "clé" d'accès au téléspectateur.
La technologie "carte à microcalculateur" utilisée lui confère toutes les propriétés dont il a besoin et ce, à un coût minimum. Enfin, elle le rend "portable" ce qui offre de nombreux avantages : ceci individualise les droits, permet l'uitilisation sur tout décodeur EUROCRYPT...
Produit de haute technologie, la carte PC2 permet la mise en œuvre des mécanismes complexes d'EUROCRYPT le plus simplement du monde.

ABSTRACT

Developing a Pay TV system requires answers to problems due to the expected pay mechanism.
To be relevant, such a system must be efficient, reliable, secured and easy to manage.
To overtake these requirements, a solution based on a removable security module, the PC2 card, has been selected. This security module stores entitlements records ans is used as a key to access programs. The micro computer card involved brings to the system all the necessary properties for a minimum price.
It makes the system removable thus providing numerous advantages, personal access rights handling, availability on any decoder...
High technology supply, PC2 allows the use of EUROCRYPT's complex mechanisms, as easily as possible.

TABLE DES MATIÈRES

1 LA CARTE PC2

La carte PC2 est la clé d'accès aux images cryptées par le système Eurocrypt. Placée dans les décodeurs, elle permet :

- *Le désembrouillage de l'image et du son* :

  La carte calcule "à la demande" les mots de contrôle qui servent au décodeur de clé pour désembrouiller l'image et le son.

  La modification permanente de ces mots de contrôle rend indispensable la présence de la carte dans le décodeur.

- *Le contrôle des titres d'accès* :

  A chaque demande de mot de contrôle venant du décodeur, la carte vérifie qu'elle dispose des titres d'accès donnant droit au programme associé au mot de contrôle. Le cas échéant, la carte enregistre l'accès à un programme et effectue le décompte des titres correspondant. Il est ainsi possible de contrôler en permanence les titres d'accès au programme en cours selon divers critères :Thème, niveau, durée, décompte de séances ....

  Grâce à la technique de désembrouillage utilisée, tous les contrôles se font en temps réel par la carte elle-même. Le décodeur est neutre vis à vis de ces contrôles.

- *La gestion des titres d'accès* :

  La carte offre un ensemble de fonctions permettant la gestion des titres d'accès par les différentes entités impliquées dans son exploitation et ce aussi bien dans des centres de distribution ou d'entretien qu' à domicile, dans le décodeur lui-même.

  Ces fonctions permettent à l'émetteur de la carte (c'est-à-dire l'entité chargée de gérer la carte dans son ensemble) la création et la suppression de services, et aux titulaires de services (généralement des fournisseurs de programme) la création, la mise à jour où l'annulation de titres d'accès.

Pour toutes ces fonctions, PC2 gère automatiquement l'ensemble des "contingences" techniques et sécuritaires qui en découlent ou qui sont nécessaires à la gestion de la carte elle-même. Ainsi les terminaux ou les décodeurs n'ont à leur charge que la gestion des données applicatives. PC2 est une carte "intelligente".

CONSEQUENCES DE CE CHOIX :

Le module de sécurité ainsi réalisé se présente sous la forme d'une carte aux normes ISO (carte de crédit), multi-prestataires, et interopérable.

Parfaitement portable et détachable, elle effectue le lien entre son porteur (le titulaire) et les titres d'accès, qui deviennent eux-mêmes portables. Il n'y a plus aucune condition d'accès associée au décodeur.

La sécurité s'en trouve accrue d'autant, et ce au moindre coût :

- La carte, réputée inviolable et impossible à copier est un véritable coffre fort pour les titres d'accès.
- Les outils de gestion de la carte permettent l'exploitation et la mise à jour des titres dans la carte elle-même, donc sans risque de falsification.
- Le décodeur n'a plus à gérer d'éléments sécuritaires ce qui en diminue les coûts et facilite leur gestion.

Enfin, les fonctions de gestion sophistiquées offertes par la carte PC2 réduisent au minimum les opérations de gestion à la charge des émetteurs de cartes et des fournisseurs de programmes.

2 FONCTIONNEMENT DE PC2

PC2 utilise principalement des outils cryptographiques pour mener à bien sa mission sécuritaire. Il faut bien retenir que la résistance à la fraude du dispositif est sa principale raison d'être et que les cartes étant largement distribuées, sans limitation de durée ni contrôle de leur "utilisation", les techniques utilisées doivent en conséquence, pouvoir résister à des attaques organisées, commises par des experts munis de moyens sophistiqués. L'utilisation du "SPOM" (décrit plus loin) et de techniques spéciales de gestion permettant d'atteindre ce but pour le stockage de données dans la carte et pour tous les traitements effectués par la carte.

Des moyens spéciaux ont été mis au point pour acheminer les données de contrôle et de gestion des titres d'accès de manière " incorruptible" depuis les émetteurs de signaux jusqu'aux cartes qui sont dans les décodeurs.

LES EMC :

Les ECM (Entitlement Control Message) servent à transporter de manière incorruptible les mots de contrôles et les conditions d'accès aux programmes associés.

1 Le mot de contrôle est transporté "chiffré". Seul un outil disposant de l'algorithme permettant le déchiffrement et d'une clé associée au service pourra restituer le mot de contrôle. Avec PC2, algorithme et clé sont résidants dans la carte et réservés à cet usage. La clé peut être modifiée en temps réel sur requête du prestataire de service.

2 Les conditions d'accès sont transmises "en clair" dans l'ECM. La carte les compare aux titres d'accès disponibles avant de déchiffrer le mot de contrôle associé.

3 Un sceau garantit l'intégrité du message reçu. Ce sceau est calculé sur les conditions d'accès et sur le mot de contrôle chiffré. Il est vérifié préalablement à tout autre traitement par la carte. Il protège ainsi le système contre toute altération des conditions d'accès associées aux mots de contrôle.

Le traitement de ces messages ECM par la carte PC2 conduit à restituer au décodeur les mots de contrôle en clair qui lui permettront de désembrouiller image et son uniquement lorsque les titres d'accès le permettent et bien sûr, lorsque la preuve de l'authenticité des messages a été établie.

LES EMM :

Ces messages (Entitlement Management Message) permettent d'exploiter les différentes fonctions de gestion offertes par PC2.

Globalement, ils sont basés sur les mêmes techniques que les ECM pour atteindre le niveau de sécurité requis :

1 Les données "confidentielles" sont transmises chiffrées à la carte : le circuit de la carte les déchiffre uniquement pour les enregistrer dans la mémoire permanente. En aucun cas ces données ne seront restituées en clair par la carte. Ceci permet la "TELE-ECRITURE" de clés secrètes, nécessaire aux mises à jour ou création de services.

2 Les messages sont protégés par un scellement qui les rend inaltérables Aucune donnée falsifiée - ou erronée - ne sera traitée par la carte.

3 Un mécanisme de sélection permet aux cartes de reconnaître et de sélectionner les messages qui leur sont destinés.

   Il est ainsi possible d'émettre des données destinées à toutes les cartes, de sélectionner un groupe de cartes voire d'envoyer une mise à jour destinée à une seule carte.

Les EMM seront utilisés pour mettre à jour les titres d'accès sans que les cartes n'aient à sortir du décodeur, pour transmettre des clés "secrètes", pour créer ou annuler des services ....

Les messages ECM et EMM suffisent pour exploiter une carte PC2 : Intelligente, la carte PC2 détermine elle-même tous les éléments techniques dont elle a besoin.

3 CONSTITUTION DE LA CARTE

La carte est constituée d'un microcalculateur "SPOM" - Self Programmable One Chip Micro Calculator - programmé par un masque adéquat, le masque PC2 inséré dans une carte plastique imprimée.

Le SPOM met en oeuvre des techniques très spéciales qui seules garantissent la sécurité finale :

- Réunion sur un seul "chip" de tous les constituants : mémoire, microprocesseur, programme, couplage.

Ainsi, il n'y a pas de "BUS" accessible entre ces éléments.

- Utilisation de mémoire ineffaçable pour les programmes et certaines données.

- Présence de bits "anti-effacement" interdisant toute tentative de corruption de la mémoire.

Ainsi, seuls les accès mémoires permis sont ceux autorisés par le programme du masque et l'utilisation de fonctions du masque (y compris les fonctions cryptographiques) est elle-même soumise aux règles programmées dans le masque.

LE MASQUE :

est le système d'exploitation implanté dans la mémoire permanente du circuit. Il en gère les différents composants, contrôle tous les accès et flux extérieurs de données. il est spécifique d'une application : PC2 est caractérisé par son masque.

Il comporte un ensemble de fonctions sécuritaires (Algorithmes, moyens de diversification, gestion de protection de zones etc...) utilisées par l'application.

PC2 gère deux types d'entités logiques :

- L'émetteur, unique pour chaque carte gère la carte (attribution ou annulation de services), possède le PIN de la carte (Personal Identification Number) qui protège certaines opérations ainsi que les données se rapportant à la carte tel que l'adresse unique etc.. Il possède une clé secrète pour effectuer ces opérations à l'aide du mécanisme d'EMM décrit plus haut.

L'émetteur peut aussi posséder une clé d'exploitation permettant le déchiffrement des ECM ainsi que des titres d'accès.

- Les services, dont le nombre n'est limité que par la place disponible (50 services sont aisement envisageables dans la première version).

Chaque service est créé par l'émetteur qui lui attribue une clé de gestion initiale. Toutes les autres données du service : paramètres, clé d'exploitation, nouvelle clé de gestion, titres d'accès sont transmises sous contrôle de la clé de gestion, par le titulaire du service lui-même.

Les fonctions principales de PC2 sont :

- Sélection des messages, contrôle d'authenticité

- Déchiffrement des mots de contrôle avec contrôle des conditions d'accès (traitement des ECM)

- Mise à jour des entités émetteur et services par télé-écriture (traitement des EMM)

- Gestion des titres d'accès au cours des opérations d'exploitation où de mise à jour.

Enfin, une extension du masque PC2 dite "Carte mère" permet de réaliser les cartes qui génèrent les EMM et les ECM dans les différents processus d'exploitation du système. Ces cartes mère offrent principalement des fonctions "réciproques" des fonctions des cartes utilisateur.

PC2 est une carte de haut niveau logique dont les ordres très simples mettent en oeuvre des ensembles complexes de services. La réalisation de fonctions complexes se trouve ainsi simplifiée à l'extrême.

4 LE PROJET PC2

L'intégration d'une carte à microcalculateur dans un système nécessite d'effectuer les étapes suivantes :

- Définition d'une architecture de sécurité et des fonctions attendues des "modules de sécurité" (étude préliminaire).

- Choix d'un composant "SPOM" susceptible d'accueillir les fonctions du module de sécurité.

- Etude et réalisation du masque, puis mise en production du masque.

L'étude préliminaire définissant les fonctions du module de sécurité peut conduire à utiliser un composant disponible "sur l'étagère" avec un masque existant.

Dans le cas de PC2, c'est de la collaboration entre Bull CP8 et le CCETT qu'est née la carte PC2. Bull CP8 a apporté son savoir faire issu de plusieurs études antérieures concernant la carte en général, la gestion d'abonnements, la télé-écriture etc...

En complément de la réalisation d'une carte, il importe de construire un système. Bull CP8 a apporté son expérience et son savoir faire dans la conception et la réalisation d'outils permettant la gestion des secrets du système, ainsi que la création et l'exploitation de cartes "de service" nécessaires au fonctionnement et à l'exploitation dudit système (cartes-mères).

Conclusion :

Le rôle de Bull CP8 dans la conception et la réalisation d'un tel système à cartes de haut niveau technologique ne se limite pas pour Bull CP8 - ni pour chacun des industriels impliqués - à la simple "sous-traitance" d'un des constituants du système. La mise en oeuvre d'un système tel qu'Eurocrypt est en fait un projet stratégique, de portée Mondiale qui fait appel à tout le savoir faire et à toutes les ressources de l'entreprise pour une participation active à la réussite du projet.

C'est à cette condition qu'ont pu naître simultanément l'ensemble des composantes du système, qui deviendra, espérons le, un standard universel.

UN NOUVEAU PROCÉDÉ D'ÉMISSION

DE CARTES MULTI-SERVICES

Didier **ANGEBAUD**, Jean-Luc **GIACHETTI**
CCETT
4 rue du Clos Courtel
BP 59
35512 CESSON SÉVIGNÉ Cedex
FRANCE
Tél : +33 99 02 46 35, +33 99 02 47 87

RÉSUMÉ

Cet exposé présente un procédé d'émission de carte à mémoire multiservices associé à un système opératoire original permettant une plus grande souplesse dans l'ouverture et la gestion de nouveaux services. Les techniques utilisées font appel aux algorithmes cryptographiques à apport nul de connaissance. Un premier prototype de carte utilisant ce procédé d'émission est en cours de réalisation. Il utilise le nouveau microcontrôleur 8-bit (83C852) de Philips Components.

TABLE DES MATIÈRES

1 L'ÉMISSION DES CARTES AUJOURD'HUI

Mais qu'est-ce donc qu'une carte à microprocesseur ? Si l'on ne prend pas en considération les caractérisques physiques de l'objet en question, la réponse est moins simple qu'il n'y paraît. Il faut peut-être formuler la question ainsi : qu'est-ce qui confère à un morceau de silicium la qualité de module sécurisé ? Bien sûr, sa capacité à protéger physiquement des secrets grâce à sa mémoire inviolable, et à effectuer des calculs cryptographiques intervient dans la réponse. Mais outre ces fonctions physiques, il en est d'autres d'ordre logique dont les principales sont :

- La fonction d'intégrité qui permet de garantir l'authenticité de la carte et l'origine des informations échangées.

- La fonction de confidentialité qui permet d'échanger secrètement des informations avec la carte.

Ces deux fonctions logiques sont notamment essentielles dans les applications à caractère multi-services.

Avant d'être réellement sécurisée, une carte à microprocesseur doit donc intégrer l'ensemble de ces fonctions et pour cela, subir trois épreuves initiatiques sans lesquelles la confiance ultérieure qu'on pourrait lui accorder serait gravement compromise :

- la fabrication
- l'encartage
- l'émission

Une dernière phase de personnalisation précède enfin la mise en circulation de la carte. Différents mécanismes de sécurité permettent le passage d'une phase à une autre. Les mécanismes mis en œuvre lors des deux premières étapes de la vie de la carte sont destinés à protéger la puce jusqu'à sa remise à l'émetteur. Ils ne sont plus actifs après l'émission de la carte : le fabricant et l'encarteur n'ont en effet aucun rôle à jouer par la suite.

Les étapes de fabrication et d'encartage permettent à la carte de disposer de l'ensemble de ses fonctions physiques, tandis que les fonctions logiques décrites précédemment sont actuellement intégrées à la carte par l'émetteur, lors de la phase d'émission. Pour cela, l'émetteur inscrit un secret appelé secret émetteur qui n'est connu que de lui.

Les techniques cryptographiques utilisées aujourd'hui reposent sur des algorithmes à clé secrète, avec une hiérarchie de clés cryptographiques secrètes. L'émetteur dispose d'une clé maîtresse. Le secret émetteur est une clé secondaire obtenue par diversification de la clé maîtresse grâce à un paramètre propre à chaque carte, tel que par exemple le n° de série de la carte ou le n° de compte de son porteur. Chaque module de sécurité dispose de la clé maîtresse pour reconstituer la clé diversifiée de la carte à laquelle il s'adresse.

Le secret émetteur permet donc de réaliser les fonctions d'intégrité et de confidentialité par application d'un algorithme à clé secrète. Dans les masques récents (PC2, MP, TB100), le secret émetteur est en fait constitué de deux clés diversifiées : la clé d'intégrité et la clé de confidentialité, permettant ainsi de séparer ces deux fonctions qui restent malgré tout sous le contrôle de l'émetteur.

L'étape d'émission telle qu'elle vient d'être décrite, présente quelques inconvénients importants dans le cadre d'une application multi-services.

En premier lieu, l'émetteur contrôle seul les fonctions d'intégrité et de confidentialité, puisqu'il est le seul à connaître les clés secrètes permettant de mettre en oeuvre ces fonctions. Par conséquent, l'authenticité de la carte ou l'intégrité d'un message émis par elle ne peut être vérifiée que par l'émetteur. De plus, cette vérification

met en oeuvre un secret essentiel qui est la clé maîtresse de l'émetteur. Or, dans une application multi-services, nous préférons une méthode de vérification publique et sans secret partagé. D'autre part, le contrôle qu'exerce l'émetteur sur la fonction de confidentialité oblige tout nouveau prestataire désirant inscrire sa première clé de service à déléguer cette opération à l'émetteur. Or, il n'est pas sécurisant pour un prestataire de déléguer, même à l'émetteur, l'inscription des premières clés de son service.

La méthode d'émission actuelle présente donc l'inconvénient de donner à l'émetteur un rôle primordial tout au long de la vie de la carte, même si une autonomie relative peut être cédée aux différents prestataires autorisés. L'objet de cet exposé est de présenter une méthode d'émission de carte permettant après cette étape d'établir malgré tout des relations directes prestataires/usagers et ce, en toute sécurité pour l'un et l'autre.

2 PEUT-ON IMAGINER UN PROCÉDÉ PERMETTANT D'ÉMETTRE DES CARTES DANS DE MEILLEURES CONDITIONS ?

2.1 PRÉSENTATION

Cette méthode pour ce faire, devrait répondre à d'autres critères que les procédés conventionnels, à savoir :

• L'émetteur est seul apte à valider la fonction d'intégrité. En revanche, la méthode de vérification doit être publique. En particulier, une carte doit pouvoir être identifiée comme telle durant toute son existence sans nécessiter la connaissance d'un secret par le vérificateur.

• La carte est autonome quant au choix du secret de confidentialité. Cette fonction n'est plus contrôlée par l'émetteur, mais par la carte elle-même. Ainsi, tout nouveau service habilité souhaitant protéger l'inscription dans la carte de sa clé secrète peut le faire sans intervention de l'émetteur.

• l'émission est une étape indispensable dans la vie de la carte mais la mise en service de celle-ci doit mettre fin à cette étape de manière définitive. L'émission devient alors une sorte d'agrément délivré par une autorité compétente. Elle peut être une opération pouvant, par exemple, être confiée à l'encarteur.

• La fonction d'intégrité peut être élargie : permettre, par exemple, à la carte de reconnaître la catégorie ou le groupe de prestataires habilités à l'utiliser. Mais ce processus ne doit pas préjuger de l'avenir et doit permettre au contraire à tout nouveau prestataire de proposer ses services à la carte sans intervention de l'autorité.

• Après la mise en service de la carte, une donnée secrète (clé ou accréditation) doit pouvoir être écrite de façon sûre en mémoire de la carte.

2.2 ALGORITHME UTILISÉ

La méthode proposée utilise la cryptographie à clé publique qui permet à deux individus de s'authentifier très simplement sans échange d'information confidentielle.

Le principal algorithme utilisé est un algorithme démonstration à apport nul de connaissance permettant de vérifier grâce à une clé publique que la carte possède en son sein une valeur secrète. Cette valeur secrète sera par la suite appelée accréditation. Il est très difficile de calculer une accréditation si on ne connait pas la clé secrète associée à la clé publique de l'algorithme. Par contre, la vérification de cette accréditation est facile. Pour des raisons de sécurité, l'accréditation doit être différente pour chaque carte et maintenue secrète.

2.3 PRÉSENTATION DE L'ALGORITHME À APPORT NUL DE CONNAISSANCE

La notion d'algorithme cryptographique à apport nul de connaissance est apparue aux Etats-Unis en 1986. Cette technique a, depuis, largement progressé et un tel algorithme implémentable sur carte à microprocesseur a été récemment breveté par Louis GUILLOU (CCETT) et Jean-Jacques QUISQUATER (Philips).

Le principe est le suivant. Dans les applications actuelles utilisant la carte à microprocesseur, toute opération cryptographique entre le vérifié et le vérificateur nécessite ou entraine la connaissance de la valeur confidentielle du vérifié par le vérificateur (soit le vérifié lui transmet cette valeur, soit il sait la recalculer).

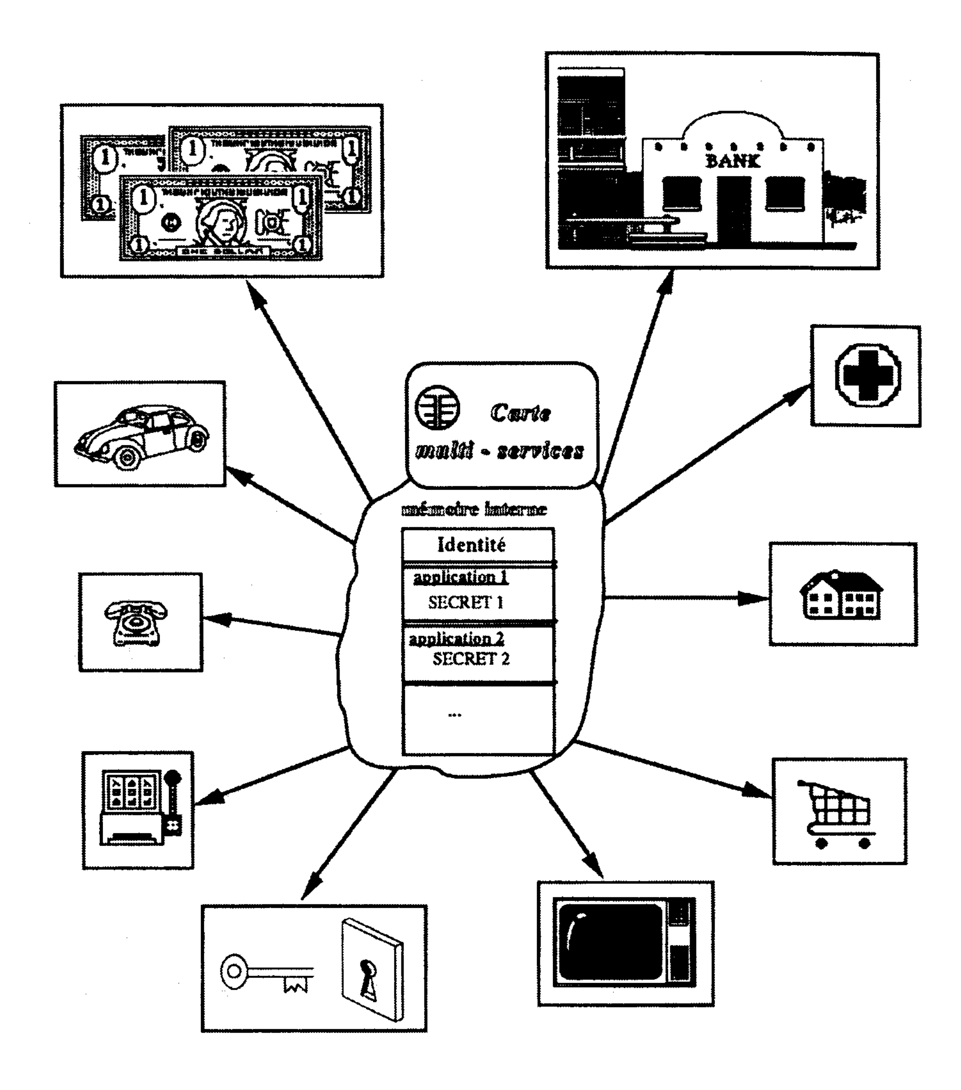
Avec l'algorithme à apport nul de connaissance, le vérificateur n'a pas besoin de connaître la valeur confidentielle du vérifié. Celle-ci n'est jamais transmise, même sous forme codée. Le vérificateur n'a besoin d'aucun secret pour contrôler le vérifié. Il y a donc moins de risques pour les valeurs confidentielles et moins de problèmes pour leur gestion.

D'autre part, l'algorithme à apport nul de connaissance permet de réaliser les schémas d'authentification (la carte de l'usager s'authentifie auprès de l'organisme ou du service souhaité), de signature (la carte signe un document pour en assurer à la fois la provenance et l'intégrité), et de multisignature (plusieurs usagers munis de leur carte signent en même temps un même document ou une information inscrite dans la carte par exemple ; la multisignature n'étant valable que lorsque tous les usagers ont signé). Il est possible également avec cet algorithme d'envisager une authentification réciproque : la carte de l'usager A authentifie celle de l'usager B et vice-versa.

2.4 CARTE MULTI-SERVICES

La carte multi-services utilisant l'algorithme à apport nul de connaissance n'est pas dédiée à une application unique. Elle peut dépendre de plusieurs autorités indépendantes, toutes placées sur un même plan d'égalité. A terme, cette carte pourra par exemple être vendue en magasin, et son propriétaire ira lui-même acquérir ses habilitations auprès des services qu'il souhaite. La notion d'émetteur disparait après la mise en circulation de la carte.

Néanmoins, il reste la possibilité d'utiliser cette carte de manière plus traditionnelle, en la limitant à une seule application.



2.5 RÉALISATION DE LA NOUVELLE CARTE

Un marché d'étude a été passé par le CCETT pour la réalisation d'un premier prototype de la carte décrite ci-dessus. Ce marché prend fin en décembre 1990. Le microprocesseur utilisé est le nouveau 83C852SC de Philips RTC disposant d'une mémoire EEPROM (c'est à dire facilement effaçable et reprogrammable) de 2 K octets. Ce microprocesseur n'est pas encore disponible sur le marché, mais le premier émulateur est disponible depuis Mai 90 et le circuit définitif est prévu pour fin 90. La maquette obtenue à l'issue du marché d'étude utilisera l'émulateur et il sera facile, à partir de là, de réaliser une carte commercialisable utilisant la version finale du microprocesseur.

Quelques chiffres :

- Fin du marché d'étude : déc. 1990.
- Date de sortie sur le marché du 83C852SC : fin 1990.
- Coût objectif du microprocesseur : <= 30 Francs.
- Durée de vie de la carte : quasiment illimitée, puisque la mémoire EEPROM de la carte peut être recyclée et reprogrammée.

3 VIE DE LA CARTE

3.1 ÉMISSION DE LA CARTE

L'état de la carte évolue alors de la façon suivante :

a - fabrication, encartage :

A ce stade, la carte se voit attribuer un numéro de série et des paramètres propres à l'émetteur (clé de fabrication). Munie de ces valeurs et après mémorisation de cet état par la carte grâce à des verrous, la carte est dite fabriquée. A l'issue de cette opération, la plupart des fonctionnalités de la carte sont bloquées. L'écriture et la lecture sont protégées.

b - émission, personnalisation :

Grâce à la clé de fabrication, l'émetteur libère certaines fonctions de la carte propres à la phase d'émission.

• Lors de la phase d'émission, l'émetteur contrôle l'inscription dans la carte des paramètres d'initialisation nécessaires. Cette opération doit être effectuée dans un local sécurisé et dans des conditions garantissant l'authenticité de la carte. L'émetteur se porte garant de son bon déroulement et en certifie le résultat. A ce stade, la carte possède, au moins, une accréditation secrète caractéristique authentifiée par l'émetteur

Se portant garant du bon déroulement de cette opération l'émetteur peut alors attribuer à la carte, une identité et une accréditation secrète associée dont la détention par la carte pourra être vérifiée ultérieurement grâce à l'algorithme GQ.

Eventuellement, l'émetteur "apprend" à la carte à reconnaître une catégorie de prestataires habilités.

Bien sûr, au passage, l'émetteur a pu configurer la carte pour un type d'application donnée et ainsi définir les limitations d'usage souhaitées.

Il reste à l'émetteur à inscrire un certain nombre d'informations telles que :
- code porteur court
- code porteur long ou alternatif.
- conditions d'ouverture de services éventuelles.

Le code porteur court est le code d'utilisation courante pour les opérations de lecture/écriture de données confidentielles ou lorsque l'accord du porteur est nécessaire pour effectuer une opération faite par un tiers (prestataire de service).

Le code porteur long est utilisé pour les opérations de réhabilitation si un blocage est désiré lorsqu'un certain nombre de codes porteurs courts faux consécutifs ont été présentés à la carte.

Une procédure de réhabilitation mettant en œuvre le code porteur court et une accréditation délivrée par un prestataire choisi par le porteur est aussi envisageable.

Les codes porteurs peuvent également être inscrits ultérieurement ou changés par le porteur, sous contrôle d'une autorité habilitée reconnaissable par la carte.

A l'issue de cette opération, l'émetteur positionne les verrous adéquats, et libère ainsi les fonctionnalités de la carte. Tous les éléments nécessaires à l'évolution de la carte sont alors présents.

La carte peut alors être délivrée ou vendue à un utilisateur. Le porteur devient le seul maître réel. Il est toutefois assujetti aux restrictions d'utilisation inscrites dans la carte à l'émission.

La carte est autonome et apte à reconnaître les prestataires habilités. L'ultime personnalisation se fera lors de l'ouverture de services.

Parallèlement, l'émetteur distribue aux prestataires habilités, présents ou à venir, une carte prestataire leur permettant d'ouvrir un service au sein des cartes émises.

3.2 MÉTHODE D'OUVERTURE D'UN SERVICE

La méthode d'émission proposée se révèle particulièrement efficace pour ouvrir de nouveaux services au sein de la carte. Le déroulement des opérations est alors le suivant :

La carte et le prestataire s'authentifient mutuellement. La carte éventuellement peut rejeter le prestataire si celui-ci ne fait pas partie de la catégorie de prestataires qu'on lui a "appris" à reconnaître.

Le prestataire ouvre une zone prestataire avec accord du porteur, si celui-ci a configuré sa carte ainsi. Il y inscrit alors :

- une identité de service comprenant éventuellement tout ou partie de l'identité porteur.
- un ensemble de droits et contrôle lié au service
- ses paramètres publics

Il calcule alors grâce à ses paramètres secrets l'accréditation du porteur dans le service puis inscrit cette accréditation en zone prestataire.

Grâce aux paramètres publics et aux accréditations secrètes inscrites dans la carte toutes les opérations sont possibles au sein d'un même service :

- authentification de la carte par le prestataire.
- authentification du prestataire par la carte.
- authentification entre cartes appartenant au même service.

Tous les calculs de certificats et signatures correspondants sont également possibles.

Les opérations de chiffrement peuvent être limitées au transfert d'information vers la carte (écriture de valeurs secrètes).

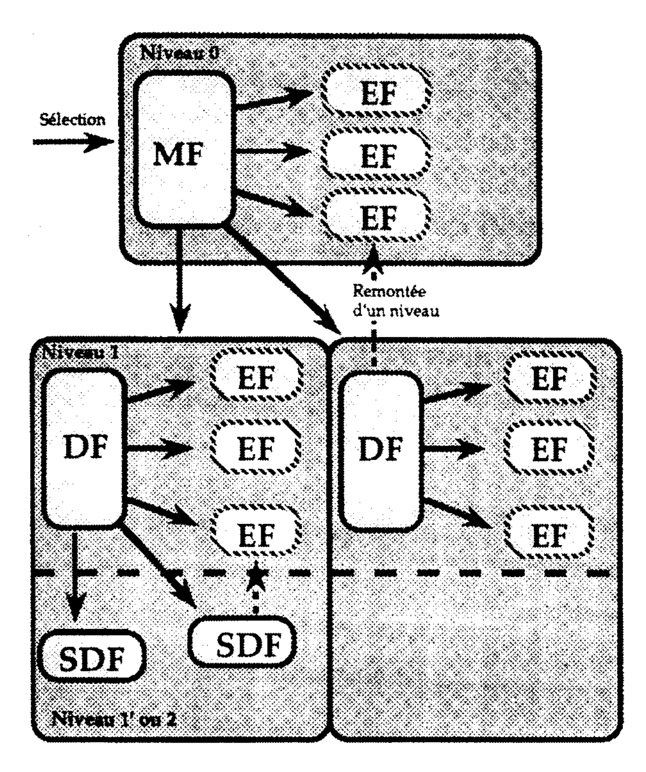
4 SCHÉMA DU NOUVEAU SYSTÈME OPÉRATOIRE

4.1 DESCRIPTION

Le nouveau système opératoire présenté tire profit de la méthode d'émission et des techniques d'ouverture de nouveaux services décrites au chapitre précédent.

L'architecture générale suit les recommandations du document ISO/IEC JTC1/SC17/WG4/N552 et N553. Elle est décrite par le schéma ci-dessous :

Structure générale



L'émission de la carte correspond à l'inscription des informations du MF (Master File). Chaque nouveau prestataire, reconnu comme tel par la carte et éventuellement sous contrôle du porteur, crée son DF (Dedicated File) ainsi que les fichiers applicatifs EF (Elementary File) dont il a besoin, en choisissant les conditions d'accès pour chacun de ces fichiers.

Les EF communs à toutes les applications sont rattachés au MF (exemple : EF contenant le code porteur long ou court, fichier géré par une fonction porte-monnaie commune aux applications ...).

Chaque application peut ouvrir un SDF (Sub Dedicated File) pour permettre à un autre prestataire de service d'accéder à ses fichiers.

Les fichiers de type MF, DF et SDF sont organisés à peu près de façon semblable.

Les fichiers de type EF sont organisés de la façon suivante:

• un en-tête constitué :
  - des conditions d'accès pour les actions décrites au paragraphe suivant,
  - de diverses combinaisons des conditions d'accès associées aux actions suivantes:
    > lecture du champ de données
    > écriture dans le champ de données (voir ci-dessous),
    > modification du champ de données
• un champ de données.

Il peut y avoir de nombreux types de EF en fonction des données qu'ils contiennent:

- code secret,
- jetons,
- accréditations,
- transactions,
- messages,
- zone de ratification,
- paramètres d'accès conditionnel complémentaires doté d'une structure plus ou moins complexe (date de validité, classe, thème, niveau).
- clés pour autre algorithme,
- etc...

L'interprètation de ces différentes données est, dans une large mesure, liée à l'application.

4.2 COMPLÉMENTS POUR LES SERVICES DIFFUSÉS

Dans le cadre d'un service diffusé, les algorithmes utilisés doivent être non-intéractifs. Les échanges dans le sens carte -> prestataire, sans être impossibles, sont en effet délicats.

Cette difficulté peut être contournée en envoyant à la carte des ordres signés par le prestataire, en s'assurant que ces ordres ne puissent être rejoués par un fraudeur. On utilisera donc l'algorithme GQ, non pas en authentification, mais en signature pour des opérations de crypto-valorisation (renouvellement de droits, modifications de paramètres publics ...).

Il est également possible de réaliser les opérations de crypto-écriture nécessaires à la distribution de nouvelles clés et accréditations, sans échange dans le sens carte -> prestataire.

SINGLE CHIP 8-BIT MICROCONTROLLER

FOR CONDITIONAL ACCESS APPLICATIONS

Henri **MOLKO**, Jean-Pierre **BOURNAS**
Philips Composants
Quai du Président Roosevelt
92134 ISSY LES MOULINEAUX
FRANCE
Tél : +33 (1) 40 93 80 12, +33 (1) 40 93 82 41

RÉSUMÉ

Couramment, dans les applications de cartes à microcontrôleur, les algorithmes sont traités par la CPU. Ceci interdit aujourd'hui l'utilisation d'algorithmes à clés publiques qui se trouve pénalisée, par des temps de calculs inacceptables, et bien souvent par l'importance de la taille mémoire nécessaire au traitement.
Une solution alternative développée par Philips Composants et PRLB consiste à associer sur le même silicium une CPU et une unité de calcul dédiée au calcul d'exponentiations et deréductions modulo n.

ABSTRACT

Currently, in the microcontroller Smart Card applications, the algorithms are treated by the CPU. The public keys algorithms have been almost impossible since the computational power of a single 8-BIT chip is weak. The computation time is too long, often the memories size are not large enough.
An alternative solution from Philips Components and PRLB integrates on same silicon CPU and a calculation unit dedicated haedware to compute an exponentiation modulo n.

TABLE OF CONTENTS

SINGLE CHIP 8-BIT CMOS MICROCONTROLLER FOR CONDITIONAL ACCESS APPLICATIONS

Henri Molko and Jean-Pierre Bournas[1]

[1] Philips Components, Quai du Président Roosevelt,
92134 Issy-les-Moulineaux, France

1 INTRODUCTION

Today, widely used in France [1], the Smart Card microchips answer perfectly to many cryptographic requirements based on secret key algorithms. But none of them are able to handle the treatment of public key algorithms [2] with the same no breaking level (key length) in a reasonnable computational time.

The increasing market demand, world-wide, of such features drive us towards the definition of a Smart Card microcontroller [3] which already support both cryptography capabilities :

secret keys and public keys algorithms.

It ends now with the design of our first secure 8-bit microcontroller for conditional access applications. Its commercial codification is 83C852.

2 PHILIPS COMPONENTS IN SMART CARD

Philips Components has for many years contributed to the development of Smart Card technology and products. In our Caen factory in Normandy we developped the assembly of Smart Cards and manufacture several types of Smart Cards and Memory Cards.

In our Hamburg, West Germany facility we also developped an integral contactless concept, basically using the same philosophy than described for ISO contact card.
Today a two chip versions is available.

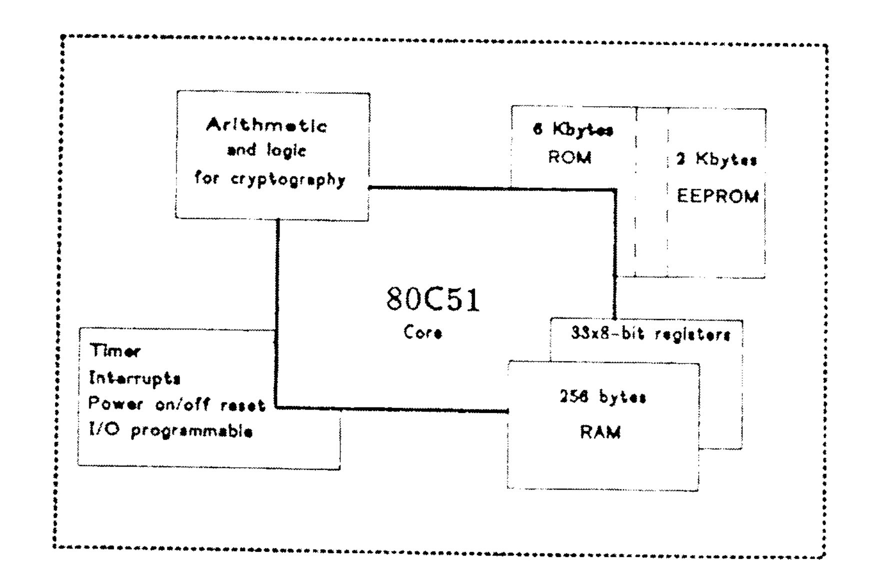
Now with its 83C852 Philips Components made a new technological step, extending the limits of the Smart Card computational power and then opening the Smart Card to new market applications.

This was possible by joining within one project group the Philips Research Laboratory's cryptography and microcontroller architecture expertise and the Philips Components' 8-bit microcontroller expertise.

On one hand the research laboratories in Brussels (PRLB) originated many original works in the field of the cryptography and security like :

- Security on large networks
- Credential management and pseudo-random numbers generator for the pay TV like CANAL+ in Belgium
- DES implementation in Philips Smart Card D1, D2 and D3
- Participation in BULL/PHILIPS Smart Card TB100
- and with the CCETT the well known **Guillou/Quisquater** Zero knowledge scheme [4].

In the other, Philips Components is one of the world leader in design and manufacture of single chip microcontrollers. Our product range is based on the 80C51 architecture for all 8 bits CPU.
The new coming **83C852** is an 80C51 family member.



83C852

3 83C852 OVERVIEW

The main features of the 83C852 are listed below :

- 8-bit CPU 80C51
- 6 Kbytes of user ROM
- 256 bytes of user RAM
- 2 Kbytes of user EEPROM
- Calculation unit
- 2 I/O lines
- Input clock frequency range : 0,5 MHz to 6 MHz
  Internal clock frequency = input clock frequency
- Single 5 V power supply
- Bond pad layout conforms to ISO specifications 7816/2

The 83C852 single chip secured microcontroller is manufactured in an advanced 1.2 µ CMOS process and has the same instructions set as the 80C51.

It has been specially designed for conditional access in secure smart card applications and provides the highest level of software and access security.
External communications are performed through a serial interface according to ISO standard. Internal memories cannot be accessed without use of the serial interface, under full control of the CPU.

The 83C852 has two software selectable modes of reduced activity for further power reduction : idle mode and power down mode.
The idle mode freezes the CPU while allowing the RAM, the timers and the interrupt system to continue functioning.
The power-down mode saves the RAM content and disables all other chip functions.

3.1 Timers

The 83C852 has two 16-bit timer registers, Timer 0 and Timer 1. The count rate is 1/6 of the oscillator frequency.

Each timer has three operating modes :

Mode 0 = 13-bit timer
Mode 1 = 16-bit timer
Mode 2 = 8-bit timer with auto-reload

3.2 Interrupt

The 83C852 has five interrupt sources, each can be programmed to one of two priority levels. The five interrupt sources are listed below :

I/O	External request from I/O lines
Timer 0	Overflow from timer 0
Cell	End of calculation cell
Timer 1	Overflow from timer 1
EEPROM	Completion of erase or erase/write EEPROM cycle.

3.3 EEPROM

The EEPROM has a capacity of 2 Kbytes. With its built-in hardware error correction, the EEPROM is a very reliable non-volatile memory. In addition to each single stored databyte, 4 extra bits for error code correction are stored in EEPROM. Single-bit errors per byte are automaticly corrected when reading the memory.

Programming of the EEPROM is completely controlled by the EEPROM's sequencer.
The EEPROM can be used either both as data memory and program memory for the CPU, or as data memory only for the Calculation Unit.
The data can only be written in EEPROM under software control contained in the ROM code area.

The main features of the EEPROM :

- 3 operating modes : byte, row, block
- Hardware error correction
- On-chip voltage multiplier
- Erase/Write cycle independant of the input clock frequency
- 10000 erase cycles per byte
- 10 years non volatile data retention
- Infinite numbers of read cycles.

3.4 Security features

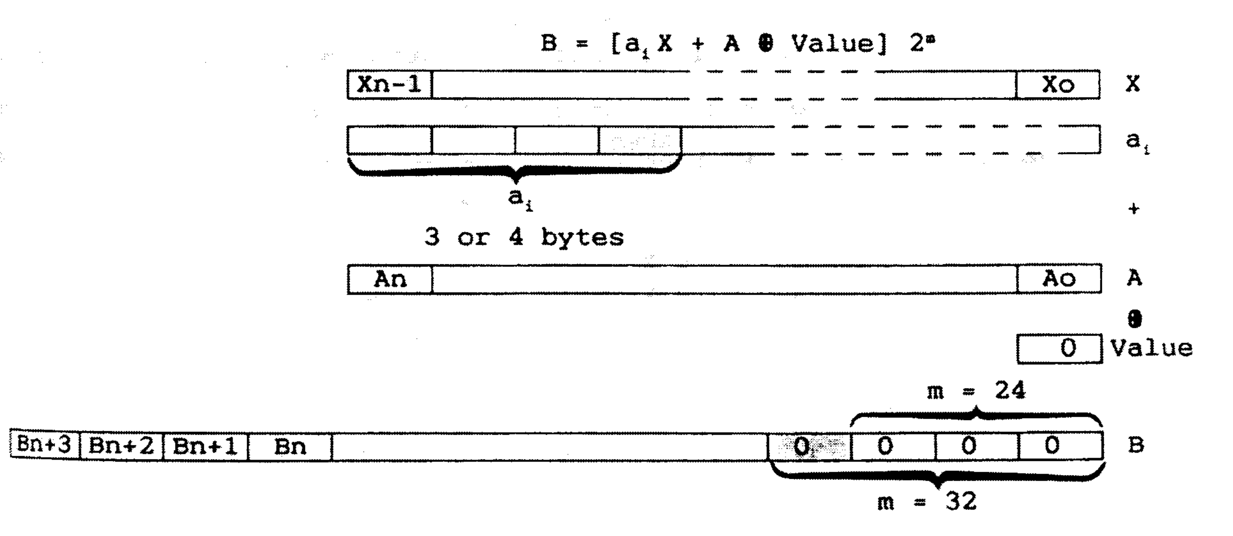
- Scrambled address bus of the EEPROM
- Hardware error correction on data stored in EEPROM
- Internal voltage multiplier
- No current examinable while EEPROM programming
- EEPROM is not self-programmable
- The probe connection to EEPROM cell bit is not possible
- Low frequency sensor
- Power supply sensor
- Two operating modes : Test mode and user mode
- Electronic fuse in EEPROM structure.
- --

4 CALCULATION UNIT

The calculation unit computes, with its associated software, any exponentiation functions like X^e mod n. It is used to enhance the public key algorithm implementations like RSA [5] and zero knowledge protocols [3,6].
For 512 bits length operands exponentiation the unit uses 196 bytes of RAM. Both calculation unit and CPU work independently. The unit accesses directly and independently of the CPU to the RAM and EEPROM memories in Read/Write modes for the RAM and only in Read mode for the EEPROM.

The calculation unit is initialized and started under control of the CPU, at the end of the total calculation, an interrupt request is sent by the unit to the CPU.

General operation of the calculation unit :



a_i has 3 or 4 bytes length and is an extract of a large number (n bytes length).
Each input operand can have n bytes length with maximum of 256 bytes.
The operands can be stored in RAM memory or in EEPROM memory.
A byte write is performed each :

- 3 periods of the internal clock if a_i = 3 bytes
- 4 periods of the internal clock if a_i = 4 bytes

General formula for the calculation time is :

For a_i = 3 bytes	For a_i = 4 bytes
(3t x nb byte write)+mt+5t	(4t x nb byte write)+mt+6t

t= period of the internal clock

Example :

For : X = 64 bytes
a_i = 3 bytes with Fclock = 3.57 MHz : 57.3 µs
A = 64 bytes with Fclock = 6.00 MHz : 34.5 µs
m = 0
B = 67 bytes

with 6 MHz the calculation unit computes

2 x 10^6 multiply/addition per second

These operations are equivalent of about 50 million instructions per second (MIPS) when using a standard 80C51 microcontroller with software solution.

Thanks to an original algorithm which has been developped by **J.J Quisquater** [7] (PRL Brussels) the calculation unit works at its optimum capabilities.
In this configuration it performs :

$X^e \bmod n$
< 1.5 s with input clock frequency = 6.00 MHz
< 2.5 s with input clock frequency = 3.57 MHz
with X, e and n 512 bit length.

Moreover, the calculation unit permits fast execution of many useful operations (see ref [8]).
Typical examples are :

$B = (a \cdot X + A) \oplus X$
$B = (a \cdot X + A) \oplus$ value

- Multiplication, addition and shift :

$B = [(a \cdot X + A) \theta 0]\, 2^m$

- Memory Initialization :

$B = (a \cdot 0 + 0) \oplus$ Initial value *(B = Initial value)*

- Data transfer :

$B = (a \cdot 0 + A) \oplus 0$ $(B = A)$

- Shift (up to 4 bytes) :

$B = (a \cdot 0 + A) \oplus 0$ $(B = A2^m)$

- Logic complement :

$B = (a \cdot 0 + A) \oplus$ FFh $(B = \overline{A})$

- Exclusive OR

$B = (a \cdot 0 + A) \oplus X$ $(B \oplus A)$

The result B has a max. length of 256 bytes or 2048 bits

A complete exponentiation (512 bits length operand) is performed with approximately 100 bytes of ROM code.

A fast XOR of large operands is useful, for instance, to enhance DES implementations.

REFERENCES

[1] L.C. Guillou, M. Ugon, *"Smart Card : a highly reliable and portable security device"*, Proc. of CRYPTO '86, Lecture notes in computer Science, Springer Verlag, Vol. 263, pp. 464-489, 1987.

[2] W. Diffie, M. Hellman, *"New directions in cryptography"* IEEE Trans. Informat. Theory, Vol. IT-22, pp. 644-654, Nov. 1976.

[3] J.-J. Quisquater, D. de Waleffe and J.-P. Bournas, *"CORSAIR : A chip card with fast RSA capability"*, Proceedings of Smart Card 2000, Amsterdam, 1989, to appear.

[4] L.C Guillou, J.-J. Quisquater, *"A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory"*, Proc. EUROCRYPT '88, Lecture notes in Computer Science, Springer Verlag, Vol. 330, pp. 123-128.

[5] R. Rivest, A. Shamir, L. Adleman, *"A method for obtaining digital signatures and public-key cryptosystems"*, C. ACM, Vol. 21, No. 2, pp. 120-126, 1978.

[6] A. Fiat, A. Shamir, *"How to prove yourself : practical solutions to identification and signature problems"*, Proc. of CRYPTO '86, Lecture notes in Computer Science, Springer Verlag, Vol. 263, pp. 186-194, 1987.

[7] J.-J. Quisquater, *"Fast modular exponentiation without division"*, manuscript.

[8] D. de Waleffe, J.-J. Quisquater, *"Architecture of a cryptographic coprocessor"*, in preparation.

ST16xyz

A FAMILY OF SECURE MICROCONTROLLERS

Laurent **SOURGEN**
SGS THOMSON Microelectronics
Zone Industrielle BP 2
13790 ROUSSET
FRANCE
Tél : +33 42 25 89 40

ABSTRACT

The ST16xyz family is a set of single chips 8 bits microcontrollers, with on board electricaly erasable non volatile memory. They have been designed for direct ISO smart card application, with a 1,5u CMOS technology. Memory sizes are modular for RAM, ROM and EEPROM to fit with application requirements. Specific hardware and firmware security features have been included in these products to monitor operating conditions and possible attempts to fraude the application.

RÉSUMÉ

La famille ST16xyz est un ensemble de circuits microcontrôleurs 8 bits monolithiques contenant une mémoire non volatile programmable et effaçable électriquement. Les circuits ont été conçus en technologie CMOS 1,5u pour les applications de cartes à puces conformes à la norme ISO. Les capacités des mémoires RAM, ROM et EEPROM sont ajustables pour s'adapter aux besoins des applications. Des dispositifs de sécurité sont inclus dans ces produits pour surveiller en permanence les conditions d'utilisation et prévenir toute tentative de fraude.

TABLE OF CONTENTS

1. CIRCUIT ARCHITECTURE

The circuit architecture is based on a modular structure to allow quick and simple design for the differents products of the family. The integrated circuits are built using five majors blocs, all interconnected through the main system bus. These five blocs are the following:

* The chip core, including an 8 bits CPU, working with a basic internal cycle of 200 ns for a 5 MHz external clock. This CPU can address up to 64K locations which cover all memories and control registers. A software controlled serial I/O plus specific security and control logic complete this master block.

* The volatile memory (RAM) which capacity can be adjusted from 96 up to 512 bytes by step of 64. This memory use a static 6 transistors cell.

* The factory programmed memory (ROM) which capacity can be sized from 1K up to 16K bytes by step of 512 bytes. An extra 1K bytes is always added for self-testing capability.

* The electrically erasable non volatile memory (EEPROM) which capacity can be sized from 64 bytes up to 3K bytes by step of 64 bytes. Parallel programming or erasing is possible up to 32 bytes in 3 ms. Programming or erasing voltage in internally generated.

* A secure parallel interface provide to the external world addresses, data and control signals like a standard microprocessor, except than these signals are controlled through internal software for secure operations. This master option is not normally used for smart card dedicated devices.

Circuits built with these blocks require only 5 connections (2 for power supply, Clock and Reset signals and the serial I/O line) as defined by ISO. Parallel interface require up to 25 more lines to provide all external signals. Figure 1 shows the generic block diagram of the family.

The memory addressing space have been divided into major areas for RAM, ROM and EEPROM. The control registers are all memory mapped for easy access. Figure 2 shows the main memory and register mapping.

FIGURE 1. BLOCK DIAGRAM

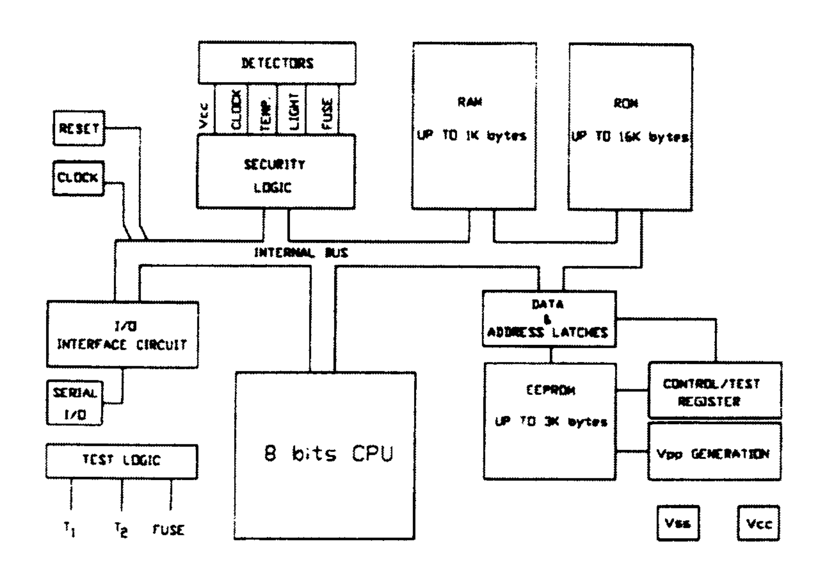


FIGURE 2. MEMORY AND REGISTER MAPPING

MEMORY MAPPING

Address	Region
0000h	REGISTERS
0020h	RAM
01FFh	Not used
2000h	TEST ROM
23FFh	Not used
4000h	USER ROM
7FFFh	Not used
E000h	EEPROM
EBFFh	Not used
FFFFh	

REGISTER MAPPING

Address	Register
0000h	I/O control
0001h	SECURITY
0002h	Not used
0003h	EEPROM Control
0004h	FUSE Control
0005h	EXTERNAL MEMORY
0006h	RANDOM NUMBER A
0007h	RANDOM NUMBER B
0008h	EEPROM TEST
0009h to 001Fh	Not used

2. SECURITY FEATURES

Security aspects cover four areas which may be listed as follow:

- Hardware operating conditions
- Internal software and data protection
- External communication and authentication
- Testing modes

2.1 OPERATING CONDITIONS.

Different hardware operating conditions are necessary to have a garanteed behaviour. Differents parameters are controlled during chip operations. Most of these sensors have no direct harware effect but results are given to the programmer through a security register which contains flags corresponding to the detected condition. A temporary condition remains detected as this register can only be reset by software.

2.1.1 SPECIFIED PARAMETERS

An integrated circuit requires some specific conditions in order to work as specificied by the manufacturer. The basic ones are:

- Power supply (for exemple 5V +/- 10%)
- Clock frequency (Minimum / Maximum)
- Temperature range (for exemple -20°C to 70°C)

If the circuit is operated outside these limits one cannot garantee that the circuit will behave as it is supposed. This is especially true for non volatile memory where the quality of programming or erasing is directly linked to those parameters. This means that the retention or number of cycling specified by the manufacturer may not be achieved.

2.1.1.1 POWER SUPPLY

The normal operating range is 5V +/- 10%. Sensors have been set to detect Vcc supply going above 5.5V or below 4.5V. Tolerance on sensor is about 1V, so it is garantee than any Vcc below 3.5V or above 6.5V will be detected as abnormal condition. This will only set the Vcc flag in the security register. The circuit is nevertheless operating correctly above 6.5V and below 3.5V. A second level of detection is done around 2.5V by a Power-Up or Power-Down device which reset the circuit as below this value the behaviour cannot be controlled. Figure 3 shows those operating limits.

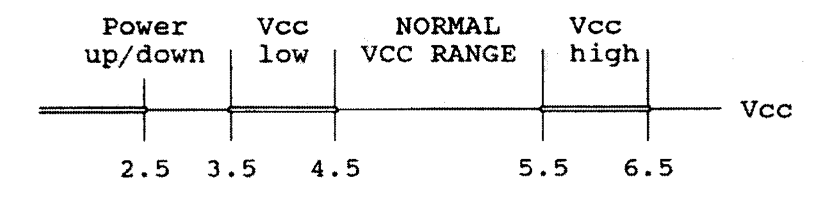


FIGURE 3. Vcc LIMITS

2.1.1.2 CLOCK FREQUENCY

The clock frequency on these circuits is limited on high frequency due to device limitation with a garanteed minimum at 5 MHz. As it is a full static design it could work down to 1 Hz or less. To avoid to easy analysis (Using a step by step clock) a minimum limit have been set to an external clock frequency of 1 MHz. Tolerance on sensor is about 750 KHz, so that anything below 250 KHz will be detected. This sensor set the CLOCK flag in the security register, and also, by hardware, inhibit all program or erase commands for the EEPROM, as timings might not be safe. Figure 4 shows those operating limits.

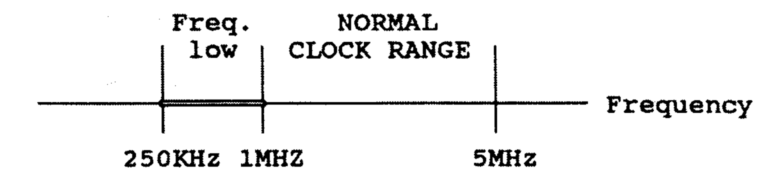


FIGURE 4. CLOCK LIMITS

2.1.1.3 TEMPERATURE

The temperature range of these circuits is normally -20°C to +70°C. Operating with higher temperature will decrease performance and does not allows to garantee programming reliabilty for the EEPROM memory. Lower temperatures are not really critical, so a single high temperature sensor have been introduced. Its detection range is about 40°C from 85°C to 125°C. Detection of such condition will set the TEMPERATURE flag in the security register. Figure 5 shows these limits.

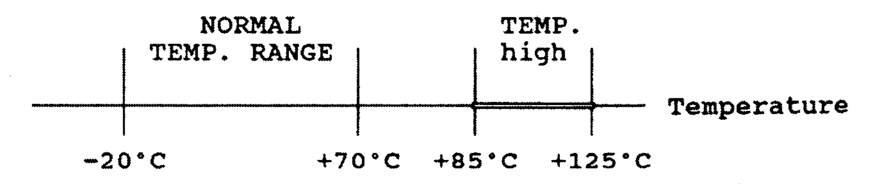


FIGURE 4. TEMPERATURE LIMITS

2.1.2 PHYSICAL CONDITIONS

The integrated circuit, in order to operate safely, must be kept in his package without alterations. Fraud attempts will require to open the normal opaque package and eventually to probe the circuit, to remove the final protection layer known as passivation. Two sensors have been included in the circuit to detect if the circuit is operating on day light or if the passivation layer have been removed. Any of these conditions will set the PHYSICAL flag in the security register.

2.2 INTERNAL DATA PROTECTION

In order to get access to data and program contained within the circuits, three potential ways exist; A software way, an electrical way and a physical way.

2.2.1 SOFTWARE PROTECTION

If the EEPROM or RAM memories are executable memory, one can imagine to download routines to try do dump secret memory contents. For that reason, the memory space have been divided into 5 major areas, one for RAM, one for USER ROM, one for test ROM, one for EEPROM and one for external memory, if any. A customer defined access matrix authorize or not one instruction of a given area to access or not data contained in given area. For exemple a subroutine in the EEPROM might be allowed to access data in RAM or in EEPROM but not in the USER ROM. Note than if EEPROM cannot access data in the EEPROM area, EEPROM becomes a non executable area. These checks are performed for every instruction fetch. This access matrix is coded at factory level like USER ROM contents.

2.2.2 ELECTRICAL PROTECTION.

When reading internal memory, it might be possible through supply current monitoring to gain some information about the quantity of logical "0" or "1" contained in the read byte.This is potentially possible either for ROM or EEPROM. To avoid such risk any time a byte is read in non volatile memory, an extra current corresponding to 3 extra bit set randomly to "0" or "1" is added. In this condition reading many times the same location will gives always different current reading. To even garantee a better data retention for EEPROM a special reading mode with shifted reference has been added in order to verify with some margin the programmed bit.

2.2.3 PHYSICAL PROTECTION

If the circuit is taken out of its package, a visual analysis can be done to try to detremine the contents of non volatile memory. In the EEPROM, data are stored through positive or negative charges trapped in a floatting gate. Up to now, no physical reading of such information is possible. In the ROM the information is coded during fabrication, and will be coded with a layer (implant layer) which cannot be read directly. One must first remove some other layers and perform a complex chimical treatment. In order to make access even more difficult the physical and logical addresses of the bits are scrambled on a 512 bits matrix.

To protect data against full U.V. or others radiations, the first 32 or 64 bytes of EEPROM can be made one time programming only to be kept as a reference for future reading.

2.3 EXTERNAL COMMUNICATION

Two different aspects have to be covered. External communication through either the single serial I/O line or through parallel interface. The second point to be covered is authentication of such devices.

2.3.1 SERIAL I/O LINE

Serial I/O data protection relies on two features. The first one is that the circuit is always the master in commmunication receiving input only when its internal program allows it. The second point relies mainly on data encryption, and in that case computing power is the best help the hardware can give. Anyways most of the proposed algorythms relies on hudges polynomials operations, and studies are now started on a specific operator to be included in the basic architecture. This will boost performance especially in public key algorythms (RSA like).

2.3.2 PARALLEL INTERFACE.

Parallel interface is completely software controlled. A specificed register is used define for each area (RAM, ROM, EEPROM) is the memory to be used is internal or external. Added to that there is a master bus control bit which only activate external bus buffers when set. When the circuit is powered up this register is initialised as all internal memory and external bus locked (All buffers in high impedance mode). In this condition only internal program can select to access external memory and there is now way to force any thing from the outside.On top of that the memory access control matrix can be used to deny access from external memory to any sensitive area inside or to make external memory as data only.

2.3.3 AUTHENTICATION

Authentication of the cards relies today on software controlled operations through different types of algorythms. Most of them require good random number for proper results. For this reason two eight bits random number generators have been included in these circuits, based on a combination of polynomial and hardware generation. The combination of the two give high quality random number much faster than usual software pseudo random number generation. Starting sequence for these random number generator has been fully characterised in order to garantee the quality of the firt try, as application often start by an authentication sequence.

2.4 TEST MODES

As these products are used mainly for high volume card applications, testing must be fast, for cost reason, and secure to garantee the quality. This implies use of specifics test conditions. The global test is done in three steps:

First the two eight bits random number generators are configured as shift registers and tested by shifting patterns.

Second, the same two eight bits generators are used to perform a full CPU test going through all instructions and producing a 16 bits signature read out by shifting out the bits as done in step 1.

Third, when the CPU is validated, a self test program tests all remaining circuits, checking registers, I/O, memories.

The selftest is activated only when the chip is in test mode. Test mode is protected with a physical fuse which can be blown once into an irreversible locked state. Fuse status can be controlled on line through one of the register bit. In addidtion a selflocking register bit provide the same hardware protection. This bit can be set during the reset sequence and then will remains set until a power off.

Selftest program will never gives direct access to ROM contents as it only outputs through the standard I/O line specific checksums. The selftest usage can be protected by a test password.

3. CONCLUSION

This family of products cover a wide range of applications, even highly secure applications. They can be used for smart card products or also to build security modules. They are well protected against fraud attempts and physical stresses including E.S.D well above standard. The general purpose member of the family, called ST16612, has 6K bytes of user ROM, 160 bytes of RAM and 2K bytes of EEPROM.

A PAY-PER-VIEW EXPERIMENT

USING D2 MAC/EUROCRYPT

Wolfgang **BOCK**
Anitra Medienprojekte
Stuntzstrasse 33
D-8000 MUNICH 80
RFA
Tél : +49 89 916392

ABSTRACT

The layout of a pay-per-view experiment using D2 MAC and Eurocrypt is given including a description of the proposed man-machine interface, cable head end and consumer hardware. Emphasis will be placed on the needs of narrowcast program providers. This experiment has been designed for being carried out on a german cable network.

RÉSUMÉ

On décrit une expérience D2 MAC/Eurocrypt de télévision avec paiement à la séance : interface homme-machine, hardware dans la tête de réseau et chez le consommateur. On insiste sur les besoins des chaînes thématiques. Cette expérience a été conçue en fonction des réseaux câblés allemands.

TABLE OF CONTENTS

1. INTRODUCTION

This paper outlines an intended pay-per-view experiment using D2MAC under the Eurocrypt access protocol, that is, the VISIOPASS family of descramblers. The work described here was performed under the RACE # 1070 set of projects "Testing pay-per-view in Europe".

Experiments such as this could conceivably serve as a showcase of MAC-specific advantages in software shipping: such as 16 by 9 exhibition, digital stereo sound, multiple-language shipping, and data downloading. However, the goals of our particular experiment are much more modest: they are to establish a practical beachhead for such applications on German cable.

Another goal has been minimum cost, particularly in the head end and in the production of packaging software. This is clearly of the utmost importance in a pilot application, particularly when the long-term goal is narrowcast television shipping.

It should be noted that the main components of the system to be described herein are already available. The VISIOPASS system has been developed by Philips, the D2MAC head end hardware by MATRA and both of course rely heavily on work done at the CCETT. The studio head end has been developed by a Dutch company, Regiokabel of Limburg, partially under the RACE project.

2. PPV SERVICE DEFINITION AND MODES

First, the service to be proposed is defined in more detail. The design aim is to provide as full a service as possible.

2.1 Service Definition

In line with its technical orientation, the size of the test sample will be small at a maximum of 500 households. This is an economic constraint, not a practical one. Each of these households will be equipped with a VISIOPASS descrambler and one pre-initialized card. The VISIOPASS descramblers will have modems associated with them for two-way pay-per-view operation.

The video software consists of movies interspersed with still-frame sequences, as outlined in 2.3 below.

2.2 PPV Modes

There are two modes of pay-per-view (PPV), impulse-pay-per-view (IPPV) and call-ahead-pay-per-view (CAPPV). Of these two modes, it is the IPPV mode which is most urgently needed for the experiment; in this particular instance, IPPV also happens to be more cost-effective. CAPPV is an additional option.

2.2.1 IPPV

IPPV may be realized in either of two modes. In either of these cases, the movie is broadcast unscrambled for the first 5 minutes: this is the "teaser": a VISIOPASS menu would appear throughout the teaser broadcast "KAUF DES FILMES: SENDEN" ("TO BUY MOVIE, PRESS 'ENTER'")

2.2.2 CAPPV

CAPPV is an option: it will be implemented only if there is GTA software (see 3.2.1 e) below) in operation in the test center:

a) during the times where operators man the GTA computer: when the user sees the movie advertised in a TV still frame, he may make a phone call to the cable head end in order to have his descrambler authorized for a particular movie, through the GTA

b) the consumer may walk through the appropriate VISIOPASS menu, and is guided through the CAPPV transaction

2.3 PPV Software

PPV software may consist of movies or of events, i.e. specially promoted violent sports, concerts, golf, etc. Indeed, PPV software could be even more general than that to include educational software, computer programs, etc.

However, in the short term, software will consist of movies. From a technical viewpoint, PPV "events" are treated exactly like movies, although in marketing terms they handle very differently.

2.3.1 Still Frame Packaging

Movies must be introduced and promoted somehow. A standard procedure has been the use of a live presenter; however, in a practical situation, such packaging material must run for extended periods of time and so, the presentation must be made lively to stay interesting. This contributes to cost.

We propose a different mode of packaging where the movies are embedded in sequences of still frames which are essentially computer-generated title pages with or without further video artwork such as logos, scanned stills from the movie, etc. Each frame is held for sufficiently long to make comfortable viewing/reading possible.

In particular, those still frames will feature

a) list of movies available today, with prices

b) for the next movie, a series of still frames promoting that movie including a brief synopsis, movie stills, and other artwork

The still frame sequence formed by a) and b) will run in carousel (round-robin) fashion. It may or may not be accompanied by a music soundtrack; the sound option introduces many practical, non-technical complications, and it will be omitted in a first stage of the experiment.

2.3.2 Movies

Movies will be tested across the entire spectrum, ranging from art movies to new product and including some (few) black-and-white offerings.

3. USER BASE

Two categories of user will be recruited in advance: a few dozen technically oriented users which are capable of fully exercising the hardware, of answering complex questions in panel sessions etc.; and representative users which would be expected to be less knowledgeable and probably less active.

These users must be selected in advance to facilitate card handling; indeed, in the present experimental mode of operation, the VISIOPASS will use smart cards that have been pre-loaded with entitlements to movies (note that in its operational version, the VISIOPASS can be loaded with movie entitlements from the head end). It is not planned, therefore, to take on new users as the experiment progresses; rather, in case there is sufficient interest and experimental motivation, one would install a second, third etc. batch of users.

4. GENERAL LAYOUT

The layout of the experiment is displayed in Fig. 1, and discussed below.

4.1 Cable Head End Studio

The D2MAC feed origination is largely automatic. It is basically comprised of five sections

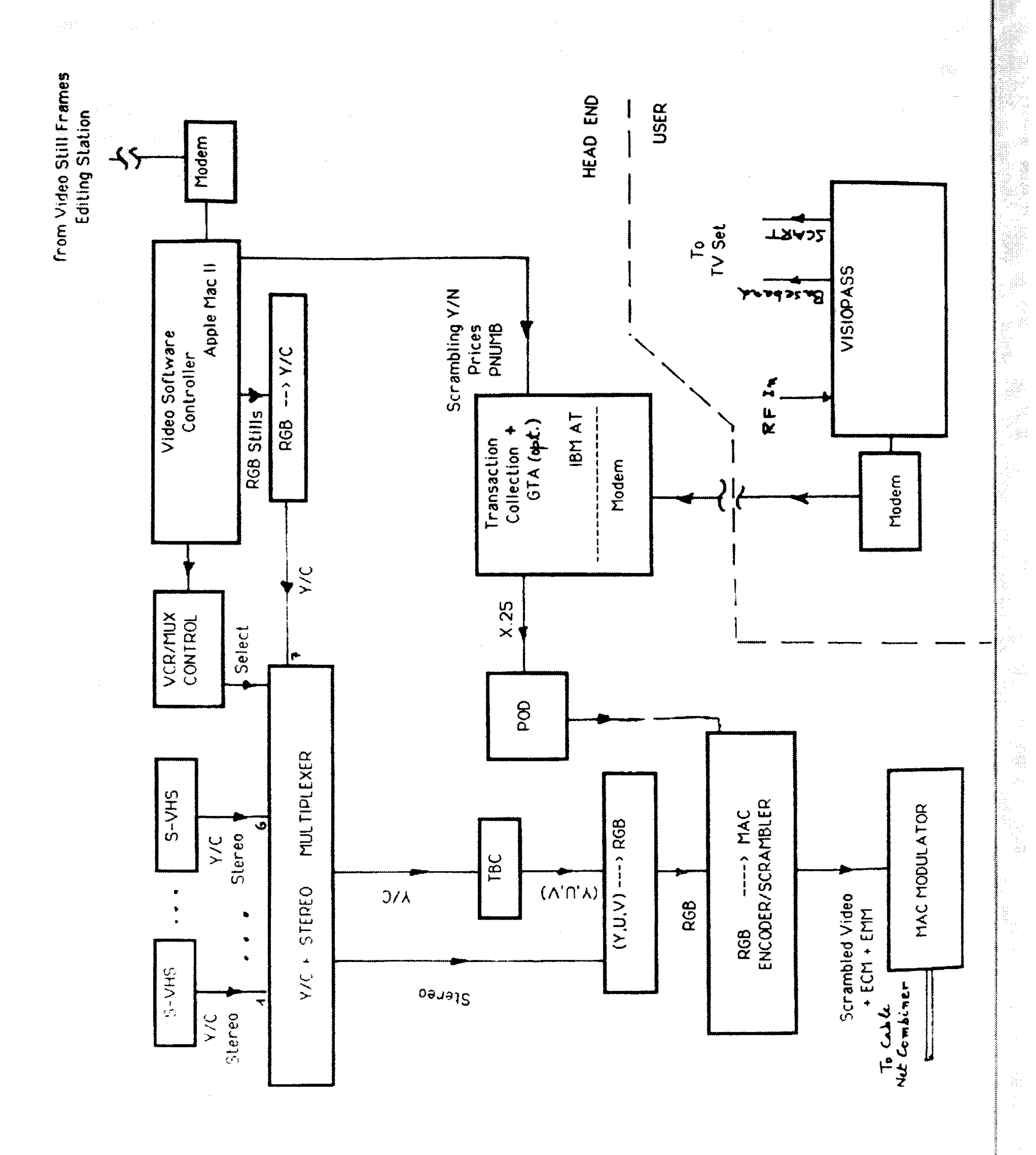


Fig. 1: System Layout

a) a <u>video still frames editing station</u>; this is not shown here. It creates data files describing promotional still frames (the movies' "packaging") in a desktop video language, and it is normally located off premises (away from the cable head end). It sends its data to a modem at the cable head end, which is connected to the video software controller

b) a <u>video software controller</u>. This is implemented on an Apple MacIntosh II, and it has three main functions

i) build an internal representation of the stills data it is getting from its modem; managing the resulting carousel of stills; outputting the correct still frame as RGB, to be converted to Y/C; the latter signal feeds the multiplexer

ii) send a control data string to the VCR/MUX control. The latter then causes the MUX (multiplexer) to select either the promotional still, or the output of one of six S-VHS VCRs; it also causes the VCRs to rewind after exhibition of a particular tape, to stand by for the next exhibition, etc.

iii) control the MAC encoder/scrambler by instructing it to scramble/not scramble; communicate the price of the movie now running, and its PNUMB program number

c) a <u>video section</u>. This consists of six S-VHS VCRs feeding a multiplexer, itself feeding a time-base corrector. Video is Y/C up to the time base corrector, which outputs a (Y,U,V) signal which is itself converted to RGB prior to being fed to the MAC scrambler, along with high-quality analog stereo sound

d) a <u>scrambling/authorizing section</u>. This consists of the D2MAC encoder/scrambler, feeding a 12 MHz MAC modulator operating at frequencies suitable for the Bundespost's hyperband channel raster.

e) a <u>transaction collection computer</u>. This IBM AT hosts a custom-written transaction collection program. That is, when the customer has entered an IPPV transaction, the corresponding PUNMB and other information is forwarded to the transaction collection programming computer at a predetermined time at night. The computer maintains a customer order file which can be exploited for billing purposes.
The GTA software (i.e. software for changing the programming tiers in the cards, for invalidating cards etc.) is optional and it would run on the same IBM PC AT.

f) a MAC scrambler and modulator. Software is of course 4 by 3 only and this is what that equipment is currently laid out for

The most salient features of this setup, apart from its use of D2MAC, are the desktop video grade program packaging (where such desktop video is generated on medium-cost equipment based on Apple MAC II platforms), and the use of S-VHS. Regiokabel Limburg has run an extensive pretest involving such a system, broadcasting in PAL on the Maastricht cable system in Holland, and we found that both the desktop video and the S-VHS quality were quite successful, not only in subjective comparison with other cable feeds, but also in the market.

4.2 Consumer equipment

Consumer equipment consists of the VISIOPASS descrambler with the appropriate card, the associated remote control, and a modem.

a) the VISIOPASS descrambler will feature German menus and a PAL modulator (but not an RF output) so that it can connect either to TV sets with a SCART connector, or to sets with a video input, but not to older sets with RF input only. The VISIOPASS will have an RF input in conformity with the German hyperband cable raster. The base bandwidth of the VISIOPASS output will be in excess of 7 MHz

b) the cards will be initialized at CCETT (if, as expected, the test does not use the GTA). The cards will be EPROM models. In case the experiment is continued, an upgrade to EEPROM cards should be possible

c) ordering will be through the remote control. The remote control will feature German captions (possibly a printed foil stuck on the remote controls)

d) a Minitel 2 type modem will be integrated into the next generation of VISIOPASS. This modem will call the transaction collection computer at a set time (in the production version, that time is set, on a consumer-specific basis, through the GTA; in the test version, each customer modem will be preset to call at a different time). The modem connects to the viewer's phone.

5. CONCLUSION

We believe a low cost head end can be built to meet the challenge of pay-per-view testing. Such a head end has all kinds of other application in software domains where low cost is paramount: such as narrowcasting, educational software, and in industrial applications.

SERVICES À ACCÈS CONDITIONNEL

SUR RÉSEAUX CÂBLÉS

Dominique **TESSIER**
Communication et Développement
4 place Raoul Dautry
75741 PARIS Cedex 15
FRANCE
Tél : +33 (1) 43 35 82 98

SERVICES A ACCES CONDITIONNEL
SUR RESEAUX CABLES

COMMUNICATION-DEVELOPPEMENT est concerné à plus d'un titre par les choix à faire en matière d'accès conditionnel sur les réseaux câblés :

- en tant d'exploitant : la règlementation française veut que la commercialisation des services de télévision câblée soit confiée aux sociétés opératrices . Pour être techniques, les choix des dispositifs d'accès conditionnel sont donc avant tout des choix de mode d'approche du marché dont ces sociétés ont la responsabilité.

- en tant que maître d'ouvrage : COMMUNICATION-DEVELOPEMENT est aujourd'hui présente de manière équilibrée entre les réseaux du Plan Câble et les réseaux qu'elle établit directement dans le cadre de la Loi du 30.9.86. Cette situation unique dans le paysage audio-visuel français a amené COMMUNICATION-DEVELOPPEMENT à se préoccuper très tôt de choix techniques engageant sa responsabilité d'investisseur-constructeur.

- enfin, à travers son engagement dans l'industrie des programmes, dont l'économie repose sur une évaluation de la taille du marché accessible à niveau de prix donné, certains programmes étant orientés "basique" et d'autres plus "option". Cet engagement a été notamment illustré récemment par l'accord que nous avons bâti avec Canal Plus et la Générale d'Images.

La complexité du faisceau de contraintes ainsi référées, comme la diversité des situations - la télévision par câble ne se vend pas de la même façon dans les stations de sport d'hiver par exemple, qu'en milieu urbain classique - nous a amenés à être pragmatiques. Dans ce cadre, les principes qui guident notre action sont les suivants :

- le "basique" reste la pierre de touche, le produit central autour duquel s'ordonne l'activité de câblo-opérateur.

- les programmes payants optionnels doivent être sélectionnés avec soin ; leur thème doit être porteur ; leur prix de vente doit se situer - s'agissant de produits qui viennent d'ajouter à un basique vendu 100 F. et plus - dans une plage d'acceptation qui nous paraît être sensiblement en dessous de 100 F. par mois. C'est ainsi que la chaîne de cinéma que nous allons proposer, en association avec la Compagnie Générale d'Images et Canal Plus, ne devrait pas coûter aux abonnés plus de 60 à 70 Francs par mois.

- les dispositifs techniques doivent coûter le moins cher possible !
Dans la mesure où ils ont vocation à donner accès à des options diverses, de prix très variés, un système de financement de type pourcentage sur la recette dégagée paraît le plus approprié.

COMMUNICATION-DEVELOPPEMENT n'a exclu a priori aucune solution technique :

- filtres, dont il faut redire qu'ils constituent encore aujourd'hui le moyen majoritaire de distribution des "pay TV" aux USA, et qui ont encore de belle réserves d'évolution

- réseaux "intelligents" qui peuvent être adaptés à des milieux particuliers propices à la "télévision à la carte" (hôtels, établissements de soins, stations de vacances)

- décodeurs dont la souplesse de fonctionnement est un atout, à condition que leur coût soit compatible avec les contraintes citées ci-avant.

* * * * *

* * *

Parmi les solutions simples que nous pourrons utiliser, l'on peut citer :

- des filtres coupe-canal ;

- des sélecteurs programmables.

En ce qui concerne les filtres leurs avantages résident dans :

- l'existence d'une technique bien rôdée aux USA, où elle reste le moyen le plus répandu d'organiser la diffusion des options payantes ;

- un niveau de prix assez bas (4 à 6 $ aux USA) qui rend cette solution financièrement attractive même en tenant compte de ce que l'on filtre les non-abonnés à l'option, donc que la charge est inversement proportionnelle au taux relatif de pénétration de celle-ci.

Mais les filtres ont aussi des inconvénients , qu'il faut prendre en considération avant de généraliser leur emploi:

- c'est une solution assez rigide, donc génératrice de coûts élevés de main d'oeuvre : ceci conduit à en réserver l'emploi à des marchés caractérisés par un plan de service assez simple (peu d'options) et par une occupation stable des logements.

- ces matériels doivent être adaptés aux caractéristiques techniques du marché français, notamment aux bandes de fréquence qui y sont utilisées.

Communication-Développement a par ailleurs procédé à l'analyse des techniques de filtres "adressables" qui permettraient de lever notamment la première de ces difficultés.
Cette solution, elle aussi apparue aux USA, retient l'attention bien qu'elle ne soit pas immédiatement utilisable en raison de ses coûts trop élevés (du même ordre que ceux des désembrouilleurs SECAM).

Quant au sélecteur programmable il présente l'avantage d'être une simple déclinaison d'un équipement déjà en service auprès d'une partie de nos abonnés. On sait que le sélecteur de programmes vise à pallier les insuffisances d'une partie des récepteurs de télévision en mémorisant tous les canaux du plan de service et en donnant accès aux bandes de fréquence VHF et UHF dans leur intégralité.

Le sélecteur est dit programmable si, en outre, il est possible de lui interdire l'accès à certaines de ces fréquences ou, au contraire, de l'y autoriser. On peut ainsi loger des programmes payants dans des bandes de fréquence inaccessibles à presque tous les téléviseurs, et ne les rendre disponibles qu'aux seuls abonnés qualifiés, à qui est fourni un sélecteur dûment programmé.

C'est ainsi que, sur certains de nos réseaux, nous proposons au-delà du basique de 18 ou 19 programmes une option composée de 4 chaînes thématiques pour un prix de 50 francs environ.

* * * * *

* * *

Pour des programmes de valeur unitaire plus élevée, telle que la chaîne de cinéma pour le câble, le recours à un désembrouilleur doit être mis en balance avec les solutions plus simples et plus limitées évoquées ci-avant.

Les systèmes de cryptage/décryptage sont, comme on le sait, multiples.

L'offre industrielle en SECAM est désormais assez abondante, elle est notamment représentée par la gamme PHILIPS (DISCRET 11 et 12, TUDI 14), par THOMSON (dont le procédé VIDEOCRYPT utilisé en PAL pour le groupe SKY pourrait être décliné en SECAM), par EURODEC (dont le décodeur SYSTER pourrait être adapté aux réseaux câblés), etc ....

D'un autre côté, COMMUNICATION-DEVELOPPEMENT suit avec attention les développements engendrés par le codage en D2 MAC/P. S'il est évident que ceux-ci ne prennent leurs sens que dans la perspective du passage à la haute définition - dont le câble a de bonnes chances d'être un jour le vecteur privilégié -, l'économie de ces systèmes reste aujourd'hui délicate. Si séduisante soit-elle sur le plan technique, il reste à fixer les mécanismes de financement qui permettent de fonder une diffusion de masse de cette norme voulue à juste titre par les pouvoirs publics.

Pour reprendre l'exemple de la chaîne cinéma que nous allons proposer en option aux abonnés au câble, il faut compter au moins 20 F pour les programmes, 20 à 25 F pour la gestion des abonnés ainsi que pour l'amortissement des frais commerciaux. Reste environ 15 F par mois pour la partie technique, sur un prix de vente fixé autour de 60 Francs.

Peut-on y arriver avec les offres actuelles, celles déjà citées en SECAM ou bien les équipements proposés en D2 MAC : VISIOPASS, voire le DECSAT de Canal Plus dans une version câble ? Chacune de ces solutions a des avantages sur les plans technique et commercial, mais l'économie du câble étant une économie tendue, les aspects financiers sont cruciaux.

Or s'il est possible d'amortir un coût technique de quelques dizaines de francs sur des programmes cryptés vendus 150 Francs et au-delà, et a fortiori sur un bouquet d'options pris par un même abonné, la capacité de financement dégagée par la chaîne cinéma est comme on l'a vu beaucoup plus faible.

Une formule de pourcentage sur la recette générée par l'opérateur du câble à travers le décodeur rendrait bien compte de cette situation.

Pour trouver son dynamisme maximum, une telle approche doit bien entendu laisser au câblo-opérateur une latitude importante quant aux méthodes de commercialisation (ristournes, création de "paquets" d'options....).

* * * * *

* * *

Enfin la distribution de services à accès conditionnel suppose, en tout état de cause, que soit déterminé entre les éditeurs de programmes et le câblo-opérateur le cadre contractuel leur permettant de fixer :

- les responsabilités de chacun : la maîtrise de son "fond de commerce" est à cet égard au coeur même du métier de câblo-opérateur ; c'est à lui que revient la responsabilité de la commercialisation, de la relation avec les abonnés du service.

- la répartition des charges et de la recette.

Ces questions de prix et de répartition des responsabilités sont au coeur des discussions que nous poursuivons tout particulièrement avec France-Télécom et avec Canal Plus.

* * * * *

* * *

Il reste pour être complet à évoquer la télévision câblée "à la carte" que nous avons commencé à installer l'hiver dernier dans les stations alpines. Ce procédé, qui a eu un succès très net, repose en fait sur deux techniques :

- dans les hôtels "haut de gamme", qui souhaitent offrir à leur clientèle une gamme de prestations qui va de la télévision à la carte au baby-sitting assisté par caméra, en passant par la gestion automatique des mini-bars, le système VISICABLE + est employé.

- dans les résidences gérées par le circuit locatif, nous installons des téléviseurs adressables.

Grâce à des messages envoyés depuis la tête de réseau et multiplexés aux signaux vidéo, nous autorisons ou refusons l'accès aux différents canaux du téléviseur en fonction du niveau de service demandé et de la durée de l'abonnement : minimum une journée, maximum deux semaines.

Pour la commercialisation, nous avons fait développer des bornes-guichet automatiques qui sont placées dans des lieux publics, disponibles 24 H sur 24 et qui permettent à toute personne ayant une carte bancaire, de s'abonner pour les programmes et la durée de son choix.

Les bornes-guichet automatiques, une par quartier de la station, sont équipées du matériel suivant :

- un micro-ordinateur et son écran

- un clavier numérique

- un lecteur motorisé qui accepte les cartes bancaires à puce et à piste

- une imprimante pour délivrer le reçu

  Le client pourra dialoguer avec la borne en cinq langues au choix : français, anglais, allemand, espagnol et italien.

- il choisira son niveau de programmes (15, 20 ou 25 chaînes par exemple)

- il choisira la durée (un jour à deux semaines)

- il identifiera son appartement

- la transaction validée, il recevra un reçu

La borne est reliée à la tête de réseau qui génère automatiquement un message envoyé sur le réseau et destiné au téléviseur du client.

Pour les clients qui n'ont pas de carte bancaire sur eux, des terminaux de paiement manuel permettront de régler : en espèces, par chèque ou carte bancaire. Ces points de paiement sont également reliés à la tête de réseau pour la mise à disposition immédiate des programmes.

A la tête de réseau, un serveur gère l'application. Il contient une base de données avec l'ensemble du parc de logements équipés de téléviseurs adressables. Il gère les niveaux de programmes, les durées et fournit les journaux et statistiques commerciales.

Mis sur pied en un temps record, ce système équipe aujourd'hui les stations de ski des ARCS et des MENUIRES, où la télévision à la carte proposée par notre filiale CABLE CITEVISION a reçu dès cet hiver un accueil très favorable. Il sera offert à d'autres stations de vacances et à d'autres clients notamment dans l'hôtellerie.

* * * * *

Tels sont aujourd'hui les différents aspects de la politique de Communication-Développement en matière d'offre de programmes à accès conditionnel sur le câble.

Dominique TESSIER
Directeur Technique
20 Avril 1990

SERVICES À CONDITIONS D'ACCÈS

LE POINT DE VUE D'UN CÂBLO-OPÉRATEUR

Michel VILLANEAU
Compagnie Générale des Eaux
Division Télédistribution
52 rue d'Anjou
75384 PARIS Cedex 08
FRANCE
Tél : +33 (1) 42 66 91 50

MICHEL VILLANEAU

14 Mai 1990

CCETT/Rennes
Jeudi 14 Juin1990
9h50/10h10

Services à conditions d'accès
Le point de vue du Cablo-opérateur

La raison d'être du câble en tant que vecteur de services audiovisuels est d'assurer économiquement la distribution à domicile d'un grand nombre de programmes dans les meilleures conditions techniques de réception.

La vocation des cablo-opérateurs est d'organiser cette distribution, c'est-à-dire, au moyen du câble, de mettre en rapport l'offre de programmes et la demande des téléspectateurs, puis d'en assurer le suivi.

Aussi longtemps que la distribution se limite à la transmission de signaux disponibles gratuitement, le service à assurer est celui d'un simple transport soumis à une seule condition d'accès : le raccordement, payant ou non. Les réseaux d'antennes collectives Français, ou les réseaux câblés Belges, offrent l'exemple de tels systèmes passifs, où un abonnement généralement modeste donne accès à un ensemble de chaînes qui pourraient être reçues gratuitement par voie hertzienne.

Les choses changent à partir du moment où le câble devient de vecteur de nouveaux programmes dont sa présence suscite la floraison.

A l'inverse des chaînes hertziennes condamnées à une programmation polyvalente pour attirer sur une seule fréquence la plus large audience, ces programmes destinés au câble se concentrent sur un thème déterminé, d'où leur nom de chaînes thématiques, d'où aussi leur audience plus restreinte et la nécessité de les rendre payantes pour atteindre un équilibre économique que la seule publicité ne peut assurer.

C'est ce type de situation que l'on rencontre en Amérique du Nord, où les chaînes thématiques se comptent aujourd'hui par dizaines.

Dès lors, se pose le problème de la mise en marché de programmes diversifiés sous différents aspects : tarification, vente, facturation, encaissement, service aux abonnés, etc...

L'expérience américaine déjà bien établie, confirmée par les débuts d'expériences britanniques et françaises, montre que les chaînes du câble se classent en deux catégories :

- les chaînes de films, dont l'audience potentielle et la valeur aux yeux du Public permettent de les vendre individuellement pour un tarif de quelques dizaines de francs.

- les thématiques proprement dites, qui sont un peu au câble ce que sont les rubriques à un journal : sport, musique, reportages, etc... Ces chaînes font la substance et l'intérêt des programmes de base du câble, dont il peut exister plusieurs niveaux, selon la richesse de la palette de programmes disponibles. Leur valeur individuelle aux yeux du Public ne dépasse guère quelques francs, ce qui interdit de les vendre autrement que groupées.

Il existe enfin une dernière catégorie de produits audiovisuels : les "évènements", de tous ordres, vendus à la séance : le Pay Per View.

Quel que soit le produit concerné, il ne faut pas oublier qu'au-delà du strict problème de marketing, il existe, une fois la vente faite, un problème économique de facturation et d'encaissement.

S'agissant de très petits montants unitaires, il ne peut s'agir que de facturation groupée, c'est-à-dire regroupée avec celle du service de base.

C'est un problème que France Télécom connaît bien avec la fonction kiosque du Minitel, facturée en marginal du téléphone.

Il en va de même sur le câble, où l'opérateur doit pouvoir facturer et encaisser individuellement, au moindre coût, un ensemble de petites redevances dont il reverse leur part aux producteurs de programmes.

Dans tous les cas, le problème du contrôle d'accès se pose fondamentalement dans les mêmes termes : permettre une segmentation du marché par le moyen le plus économique compatible avec les exigences du service considéré.

Concrètement cela se traduit sur le terrain par une grande diversité de situation, de complexité croissante :

- la plus simple et la plus fréquente est celle où il existe deux niveaux de service. C'est notamment le cas lorsque le câble doit assurer un service collectif d'antenne réduit à quelques chaînes et un service d'abonnement individuel à un programme de base plus étoffé.

  Dans ce cas, une tarification typique en France est de 20F pour le service d'antenne et de 140/150F pour le service de base. Aux Etats-Unis une tarification typique à 2 niveaux est de 60F pour un basic de 15/20 canaux et de 120F pour 25/30 canaux.

  Le filtre est la solution technique à la fois la plus simple et la plus économique pour ce type de distribution à deux niveaux.

- Une situation plus complexe est celle où l'on offre, outre 2 ou 3 niveaux de services de base, des options payantes telles que des chaînes de cinéma.

  C'est le cas de la grande majorité des réseaux américains et britanniques. En France, les contraintes imposées par une programmation encore embryonnaire, ainsi que par une capacité généralement encore insuffisante des réseaux, conduit à limiter pour le moment le recours à ce type de segmentation.

  Toutefois, là où la capacité de transport est suffisante, une segmentation judicieuse permet de mieux répondre aux attentes de la clientèle.

  Les solutions techniques pour assurer cette segmentation peuvent être diverses : sélecteur programmé (comme à Sète), embrouilleur/désembrouilleur à combinaisons multiples pré-programmées (comme à Monaco), commutation (comme à Nice et dans le Nord sur les réseaux de Région Câble ou comme sur les réseaux 1G de France Télécom).

- Enfin, lorsque l'on veut assurer un service de Pay Per View, il faut organiser une inter-activité, laquelle peut prendre diverses formes.

  La plus répandue actuellement reste l'ouverture d'un canal au moyen d'un terminal adressable à partir de la tête de réseau, sur appel téléphonique de l'abonné.

  Les systèmes modernes dit "Impulse Pay Per View" permettent désormais l'inter-activité directe à travers le terminal.

C'est notamment le cas avec les réseaux commutés Cabletime utilisés par le Groupe Générale des Eaux sur ses réseaux concessifs en France et au Royaume-Uni.

Les Américains sont de leur côté en train d'équiper leurs réseaux arborescents de terminaux à impulsion.

Enfin, il faut souligner que le programme Visiopass de France Télécom vise au développement d'un terminal adressable inter-actif permettant d'assurer l'ensemble de ces fonctions.

On voit que la gamme des situations et la palette des solutions techniques sont extrêmement larges. Encore une fois, l'opérateur ne doit pas confondre les buts et les moyens :

- le but, c'est de satisfaire le client en lui offrant un choix de menus à des tarifs modulés.
- la réponse technique c'est le contrôle d'accès.

La contrainte économique, c'est que ce contrôle ne doit pas peser sur le prix du service. En pratique, le coût du terminal d'abonné ne doit pas excéder 10% du montant de l'abonnement, ce qui situe le coût du contrôle d'accès au maximum à 15F/mois/abonné pour un terminal polyvalent et autour de 1,50F par canal pour un système de filtrage.

Sous ces réserves, le contrôle d'accès doit-être considéré comme un élément essentiel à l'activité du câble, dont il conditionne l'utilisation rationnelle et harmonieuse.

LES ACTIONS DE FRANCE TELECOM

DANS LE DOMAINE DES SERVICES

À CONDITIONS D'ACCÈS

Enjeux économiques et perspectives techniques

Jean-Pierre COUSTEL
FRANCE TELECOM
Service des Télécommunications de l'Image
6 place d'Alleray
75740 PARIS Cedex 15
FRANCE
Tél : +33 (1) 44 44 22 22

ABSTRACT

FRANCE TELECOM, the Public Telecom Operator in France, has launched at the end of 1988 an ambitious program of conditional access services development. Those new conditional access capabilities will enable the Program Providers to present viewers with paying television services on a large scale. These will be developed in D2-MAC/Packet with the EUROCRYPT conditional access system, on DBS satellites as well as on cable systems, granting the user single box operation. The first services are to be in operation by June 1990 for the programs broadcasted by TDF1, and services on cable systems will be available for commercial development by October 1990.

The paper addresses the French Public Telecom Operator's strategy and expectations, and highlights the views of FRANCE TELECOM that conditional access services are the necessary step towards future and promising new television services.

LES ACTIONS DE FRANCE TELECOM DANS LE DOMAINE DES SERVICES À CONDITIONS D'ACCÈS
Enjeux Économiques et Perspectives Techniques

Jean-Pierre Coustel, FRANCE TELECOM

Opérateur public des services de télécommunications, FRANCE TELECOM exploite les infrastructures sur lesquelles sont distribués les programmes de télévision ; l'action a été très intense sur la période récente pour le développement des réseaux câblés (75% des réseaux français en 1989), et des systèmes de télévision sur satellite (pour des services grand public sur TDF1 aujourd'hui, et de futures applications sur TELECOM2 à partir de 1992). Avec le concours de sa filiale TDF, dont l'activité a traditionnellement porté sur la diffusion hertzienne, c'est désormais sur l'ensemble des moyens de télévision que FRANCE TELECOM peut intervenir.

A l'exception des programmes de CANAL+, le télespectateur correctement équipé a librement accès à tous les programmes disponibles sur ces réseaux de diffusion. Cela peut être en réalité très coûteux pour le téléspectateur (comme dans le cas des réseaux câblés où dans la plupart des cas, il reçoit sans pouvoir choisir un grand nombre de programmes), cela oblige de plus en plus la société de programme à recourir au financement publicitaire (et limite d'autant l'attrait des programmes), cela rend très difficile l'entrée de nouvelles sociétés de programmes sur le marché (comme le montre le coût d'équipement en teminaux dédiés pour un réseau de trois millions d'abonnés tel que celui de CANAL+ actuellement), et enfin, cela répond mal aux besoins des producteurs d'images, pour qui un bon système est celui qui permet de connaître exactement les volumes consommés, et qui favorise en même temps l'installation de nouveaux circuits courts de commercialisation.

LA NÉCESSITÉ ÉCONOMIQUE DES SERVICES À CONDITIONS D'ACCÈS

Pour résoudre cette situation dans laquelle la quasi-totalité des acteurs n'est pas satisfaite, et avec l'objectif général de susciter l'épanouissement de nouveaux services de télévision grand-public, FRANCE TELECOM a lancé à la fin de l'année 1988 un programme ambitieux d'installation sur ses infrastructures des capacités techniques sur lesquelles ses clients, fournisseurs de programmes de télévision, développeront à leur tour de futurs services de télévision à péage. Cet engagement a pris concrètement forme à la fin du mois d'avril 1989 avec la commande au groupe PHILIPS de 750 000 terminaux désembrouilleurs VISIOPASS.

FRANCE TELECOM n'a pas l'intention d'agir dans le domaine du contenu, et ses motivations, en tant qu'opérateur public de télécommunications et de télédiffusion, se situent essentiellement sur un plan économique. FRANCE TELECOM a la certitude en

effet que les services de télévision à péage auront une place de plus en plus grande dans l'avenir de la télévision ; les fonctions de contrôle d'accès seront techniquement indispensables pour compléter les investissements considérables déjà engagés par FRANCE TELECOM dans les infrastructures de réseaux câblés et de satellites ; l'objectif de progressivité de l'offre et de son coût pour le consommateur rend nécessaire de pouvoir commercialiser les services en segmentant physiquement les capacités de diffusion, au contraire de ce qui a été fait historiquement dans les réseaux câblés.

La recherche de l'optimum collectif conduit à ce que les systèmes soient ouverts ; ils doivent ainsi permettre la liberté du choix du téléspectateur consommateur, tout comme le fonctionnement efficace d'un marché dont la formation résultera de plus en plus de mécanismes concurrentiels.

FRANCE TELECOM OPERATEUR TECHNIQUE DU CONTRÔLE D'ACCÈS

La solution technique retenue (signaux de télévision de grande qualité en D2-MAC et système EUROCRYPT de contrôle d'accès) est identique pour les applications sur réseaux câblés et sur satellite en réception directe. Les applications de télévision à péage qu'elle permet ouvrent l'ère de l'image à la carte, dans laquelle le téléspectateur paie volontairement ce qu'il décide de voir : ce sont la télévision par abonnement, par thèmes ou par niveaux ; la télévision à péage par programme, par réservation et surtout par achat impulsif ; et enfin, la télévision avec paiement à la consommation (proportionnel à la durée). Ces nouveaux services dont la généralisation va transformer la télévision seront développés par les partenaires de FRANCE TELECOM fournisseurs de programmes. Le métier de fournisseur de programme est de commercialiser vers le téléspectateur consommateur final le contenu audiovisuel : sous ce terme générique ont ainsi rassemblés aujourd'hui les sociétés de programmes, exploitants traditionnels des "chaînes de télévision", et les opérateurs commerciaux des réseaux câblés, qui offrent sous des formes diverses des packages de services à leurs abonnés. On devrait y rencontrer bientôt les distributeurs du cinéma qui trouveront dans ces nouvelles techniques de la télévision un moyen performant d'atteindre le consommateur.

Dans son rôle d'opérateur public, FRANCE TELECOM s'efforce de rechercher la cohérence globale,spécialement sur le plan technique, des structures cibles, et des processus de transformation qui permettront de les atteindre. Les moyens de contrôle d'accès dont l'installation dans les réseaux accompagnera ces transformations devront donc garantir la transparence des solutions retenues : la transparence est nécessaire sur le plan technique pour rendre les services commercialisés indépendants du réseau de diffusion, celui-ci pouvant être hertzien, par satellite, ou sur réseaux câblés ; une architecture d'organisation transparente garantira que les contraintes supportées par chacun des fournisseurs de programmes, notamment sur le plan économique, seront réparties équitablement.

Les solutions techniques autour desquelles s'articule le programme VISIOPASS sont porteuses d'avenir, exportables, instituables en normes internationales, techniquement valides à long terme, et économiquement efficaces : le choix du D2-MAC sur câble et sur satellite apporte ainsi de nombreux éléments de réponse, parmi lesquels l'unicité des terminaux chez le client, le recours à des ressources techniques (terminaux désembrouilleurs, cartes, systèmes de gestion) partageables, l'amélioration de la qualité, la préparation des transitions vers les solutions techniques de l'après-SECAM/PAL qui seront celles de la TVHD.

UNE INTERVENTION ACTIVE POUR UNE MISE EN PLACE EFFICACE DES SERVICES

La situation française, illustrée notamment par l'histoire récente des réseaux câblés et du projet TDF1, montre qu'il est nécessaire d'accompagner et de soutenir activement le développement des périodes. La rationalité économique encourage avec urgence un tel engagement pour ce qui concerne les services sur TDF1 et sur les réseaux câblés ; la perception du risque d'incohérence technique, notamment sur l'exemple de la situation britannique, encourage une approche sans ambigüité qui entraînera la réduction du degré global d'incertitude sur ces questions, autant techniques que stratégiques. Ainsi l'intervention de FRANCE TELECOM se situera dans les prestations techniques de contrôle d'accès, mais aussi dans les actions qui permettront la constitution rapide d'un parc de récepteurs, qui représente la part la plus élevée des coûts d'équipement.

A plus long terme l'équipement banalisé des terminaux désembrouilleurs ou de fonctions équivalentes intégrées dans le téléviseur sera entièrement pris en charge par le téléspectateur, en toute indépendance des fournisseurs de programmes, comme cela a été historiquement le cas pour les téléviseurs ; en collaboration avec les industriels du secteur, FRANCE TELECOM s'efforcera de plus que cette transition puisse se faire le plus rapidement possible, tout en respectant l'objectif initial de constitution du parc étendu qui seul permettra des applications commerciales solides.

Pour le démarrage des services, prévu en juin 1990 quand les terminaux VISIOPASS seront livrés, en volume, les modalités de l'intervention de FRANCE TELECOM dans la distribution de ces terminaux ne sont pas encore définitivement arrêtées. Elles associeront concrètement les fournisseurs de programme engagés dans le développement des services autorisés sur TDF1, et les opérateurs commerciaux des réseaux câblés ; l'action en harmonie de ces divers partenaires visera à rencontrer la confiance du télespectateur, qui sera un facteur déterminant du succès de ces nouvelles applications à l'échelle nationale.

DES PERSPECTIVES PROMETTEUSES A PLUS LONG TERME

La dimension de l'engagement de FRANCE TELECOM sur le plan technique et industriel illustre par elle-même avec clarté la portée des enjeux économiques attachés au développement des services à conditions d'accès. Mais d'autres motivations sous-tendent les déterminations ambitieuses de FRANCE TELECOM dans le programme VISIOPASS.

Parmi celles-ci, figure le soutien à la norme D2-MAC/Paquet comme vecteur du progrès de la télévision, conformément aux orientations fixées par les pouvoirs publics. Au-delà des améliorations immédiates de qualité déjà mentionnées, et sa puissance comme support des services de contrôle d'accès, le D2-MAC prépare la transition vers de futures normes de télévision à haute définition (TVHD). Leur acceptation par l'industrie, les producteurs d'images, et les téléspectateurs, sera favorisée par un développement technique qui, du côté du téléviseur, garantit la compatibilité des produits existants avec les services futurs.

Le procédé EUROCRYPT, dont les spécifications principales ont été élaborées par le CCETT, est organisé autour du concept de "processeur sécurisé détachable", au contraire de la quasi-totalité des systèmes de contrôle d'accès de la génération précédente. Cette option de structure a une importance considérable en matière de sécurité, de coût d'exploitation, et surtout, vis-à-vis de l'objectif d'ouverture. Elle est réalisée concrètement avec le moyen technique de la carte à mémoire, et se situe ainsi en parfaite harmonie avec les objectifs affichés de longue date par FRANCE TELECOM dans ce domaine. Au-delà des effets positifs d'entraînement escomptés sur le plan industriel, à l'échelle nationale et internationale, les perspectives de constitution d'un parc de plusieurs centaines de milliers d'appareils grand public équipés d'un lecteur de carte à mémoire, même s'il est sommaire, font apparaître de nouveaux avantages indirects du programme VISIOPASS, qui dépassent le domaine de la télévision. Il est ainsi très séduisant d'imaginer les fruits de la synergie que l'on devine entre VISIOPASS et les projets particuliers de FRANCE TELECOM dans le secteur du télépaiement.

Enfin, on peut citer comme autre facteur de motivation le potentiel des solutions techniques retenues pour de nouveaux services professionnels: la capacité du multiplex D2-MAC de base, en diffusion de données notamment, la facilité d'extensions vers d'autres formats de la famille MAC/Paquet, et le savoir-faire acquis dans l'exploitation opérationnelle de l'adressage de terminaux en très grand nombre, font apercevoir des

ARCHITECTURE DES POINTS D'ÉMISSION

D2 MAC/PAQUET-EUROCRYPT DE FRANCE TELECOM

Jean-Pierre **VIGARIÉ**, Vincent **LENOIR**
CCETT
4 rue du Clos Courtel - BP 59
35512 CESSON SÉVIGNÉ Cedex
FRANCE
Tél : +33 99 02 43 70, +33 99 02 46 07

Jean Claude **JOUET**
Matra Communication
rue Jean-Piere Timbaud - BP 26
78392 BOIS D'ARCY
FRANCE
Tél : +33 (1) 34 60 82 44

RÉSUMÉ

En 1990 seront mis en service par FRANCE TELECOM des points d'émission D2-MAC/ Paquet-Eurocrypt. Ces équipements industrialisés sont conçus selon deux configurations en fonction de leur exploitation sur un canal satellite ou en tête de réseau câblé.
Après un bref rappel des finalités d'un codeur-embrouilleur (producteur d'un signal D2-MAC/ Paquet en bande de base, embrouillage des composantes et prise en compte du contrôle d'accès), on présente les principes qui ont conduit à l'architecture retenue pour ces points d'émission par FRANCE TELECOM : opérateurs multiples distants, contrôle local et gestion distante des titres d'accès.
Chaque constituant de point d'émission est décrit dans ces fonctionnalités. Les deux types de configurations mises en œuvre (satellite, câble) sont comparées, en détaillant le traitement de la sécurisation de tels systèmes.

TABLE DES MATIÈRES

Le projet VISIOPASS met en oeuvre sur les canaux satellites et réseaux cablés relevant de France Télécom un système complet de télévision à péage s'appuyant sur la norme de codage D2-MAC/Paquet et les spécifications d'accès conditionnel EUROCRYPT. Un des principaux aspects de cette mise en oeuvre est le développement de points d'émission assurant le codage et l'embrouillage des signaux audiovisuels diffusés.

Après la présentation de leur rôle dans VISIOPASS, cette communication décrit en deux parties les points d'émission spécialement définis pour VISIOPASS. On présente d'une part les principes d'architecture définis et retenus par France Télécom dans la conception des points d'émission, tant pour un canal satellite que pour une tête de réseau cablé. D'autre part, on décrit la réalisation industrielle qui en est faite par Matra Communication et dont la mise en place effective a débuté en 1990.

I. LES FONCTIONNALITES DU POINT D'EMISSION.

Dans la structure globale VISIOPASS, qui est constituée de plusieurs blocs fondamentaux tels que le système de gestion commerciale des usagers ou le décodeur, le point d'émission génère les signaux à diffuser vers les décodeurs des usagers. Il reçoit donc les composantes des programmes (image, sons, télétextes) et les conditions d'accès associées, les directives de diffusion fournies par les opérateurs de programme, et les messageries de gestion des titres d'accès issues des fonctions commerciales. Il délivre sur différents canaux des signaux codés et embrouillés.

Pour générer le signal à diffuser, le système de codage et d'embrouillage retenu est le système D2-MAC/Paquet, associé aux spécifications d'accès conditionnel EUROCRYPT et au processeur de sécurité PC2. L'ensemble des fonctionnalités du D2-MAC/Paquet et d'EUROCRYPT est mis en oeuvre. En particulier, plusieurs services (TV, radio, télétexte, adressage sur antenne) appartenant à plusieurs opérateurs différents peuvent coexister dans le signal, sans autre restriction sur les composantes que les dimensionnements techniques.

Deux types de point d'émission sont développés : pour un satellite, pour un réseau cablé. En version satellite, le point d'émission fournit un signal pour un seul canal. En version réseau cablé, il alimente plusieurs canaux, le signal étant particularisé à chaque canal : la configuration maximale retenue est de 15 canaux. Ces deux versions de point d'émission diffèrent principalement par la stratégie de sécurisation de fonctionnement induite par le nombre de canaux. Vues d'un opérateur de programme, les autres fonctionnalités sont identiques.

II. PRINCIPE DE L'ARCHITECTURE DES POINTS D'EMISSION.

II.1. Génération du signal en bande de base

La fonction du point d'émission est de délivrer un signal codé et embrouillé conformément aux spécifications D2-MAC/Paquet et EUROCRYPT. Elle est assurée par un codeur-embrouilleur banalisé, générant un signal en bande de base.

Le codeur-embrouilleur reçoit les composantes audiovisuelles (images, sons, télétextes) pour l'ensemble des services d'un même canal et les messageries de gestion des titres d'accès. Il génère en interne les messageries de contrôle des titres d'accès. Il élabore le signal à diffuser selon les directives issues des différents opérateurs se partageant le canal.

Le fonctionnement du codeur-embrouilleur est tout particulièrement optimisé en ce qui concerne le comportement temporelle des composantes dans le signal vis à vis de la souplesse d'exploitation pour l'opérateur de programme et vis à vis de la réaction des décodeurs.

On notera que le codeur-embrouilleur n'a pas de sécurisation de fonctionnement intrinsèque et que son entrée "directives" est unique. Ces deux aspects justifient en grande partie l'existence du frontal décrit ci-après.

II.2. Supervision du point d'émission.

L'ensemble des codeurs-embrouilleurs d'un point d'émission est sous le contrôle d'un calculateur frontal exploité par un opérateur de supervision privilégié.

Le rôle de ce frontal est triple :

- il surveille le bon fonctionnement de chaque codeur-embrouilleur par examen de leurs alarmes internes ou par analyse de leur signal de sortie : le cas échéant, il décide le passage sur un codeur de secours.

- il gère le partage des canaux entre les différents opérateurs de programme : d'une part, il répartit les ressources (nombre de paquets, lignes de télétextes, MAC) entre les opérateurs de programme, les services et les canaux ; d'autre part, il concentre sur chaque codeur-embrouilleur les directives de fonctionnement émises par les différents opérateurs de programme dans la limite des ressources allouées.

- il peut se substituer temporairement, avec des fonctions limitées, à un opérateur de programme.

Le frontal est constitué d'une partie commande des codeurs-embrouilleurs localisée près de ceux-ci et d'un pupitre de supervision qui peut être déportable.

II.3. Accès par un opérateur de programme.

Chaque opérateur de programme peut accéder à un point d'émission par un pupitre opérateur distant ("POD"). Chaque POD est connecté au frontal par un accès de type X25 en liaison permanente ou par TRANSPAC.

Depuis le POD, l'opérateur de programme dirige le ou les codeurs-embrouilleurs qui le concernent dans la limite exclusive des ressources qui lui sont allouées par le frontal (respect du nombre de paquets/seconde, commande du MAC réservé au service TV,...). Dans ce cadre, il peut définir dynamiquement l'état de chacun de ses services, tant pour le codage de base (lois de codage sonore, embrouillage ou non...) que pour l'accès conditionnel (modes d'accès, références des clés...). L'opérateur de programme ne commande pas individuellement chaque constituant du codeur-embrouilleur, mais définit depuis le POD la "configuration" du signal de sortie pour le service qui le concerne.

Le POD est destiné à être intégré dans les équipements de production finale d'un opérateur de programme qui souhaitera l'adapter à ses propres besoins. Afin de permettre aisément cette intégration, le protocole POD/Frontal a été clairement spécifié et la couche logicielle gérant ce protocole côté POD a été réalisée pour s'inclure dans tout développement POD spécifique. Pour France-Télécom, un POD de base, s'appuyant sur cette couche protocole, a été développé pour en valider la fonctionnalité.

II.4. Traitement de l'accès conditionnel.

Le point d'émission permet de traiter les deux aspects de l'accès conditionnel EUROCRYPT : le contrôle des titres d'accès, la gestion des titres d'accès.

Le contrôle des titres d'accès est traité intégralement à l'intérieur du codeur-embrouilleur. Cette fonction assure d'une part la génération aléatoire des mots de contrôle utilisés pour l'embrouillage. D'autre part, elle reçoit des directives de chaque opérateur de programme, via le frontal, pour élaborer les messages ECM et les EMM-C de remplacement. Le processeur de sécurité (carte-mère PC2), nécessaire au chiffrement des mots de contrôle et au calcul des signatures, dispose d'un lecteur dans le codeur-embrouilleur.

La messagerie de gestion des titres d'accès est définie quant à son contenu et aux modalités de sa diffusion par un organe externe au point d'émission ("GTA", gestionnaire des titres d'accès, lié au système de gestion commerciale des usagers). Elle parvient au point d'émission dans un diffuseur de messagerie ("DM") commun à tous les codeurs-embrouilleurs et fournissant à chacun de ceux-ci les EMM selon des cycles de diffusion. La messagerie de gestion des titres d'accès est véhiculée dans le service d'adressage sur antenne de chaque canal.

II.5. Sécurisation du fonctionnement d'un point d'émission.

Cet aspect caractérise le point d'émission satellite et le point d'émission réseau cablé.

Dans la version satellite, un point d'émission alimente un seul canal. Appelé "1+1", il est constitué de 2 codeurs-embrouilleurs fonctionnant en parallèle sur les mêmes signaux à coder et selon les mêmes directives. Un de ces codeurs est à l'antenne, l'autre pouvant le remplacer à tout moment en cas de panne.

Dans la version réseau cablé, un point d'émission alimente jusqu'à 15 canaux avec des signaux différents. Appelé "N+1", il est constitué d'autant de codeurs-embrouilleurs que de canaux ("N"), plus un codeur-embrouilleur de secours. Chaque codeur-embrouilleur est affecté statiquement à un canal. Le codeur-embrouilleur de secours peut remplacer n'importe quel autre après qu'on a commuté les signaux à coder et le signal de sortie et après que les directives en cours du codeur-embrouilleur en panneont été chargé dans le codeur-embrouilleur de secours.

Ces deux versions de point d'émission ont les points communs suivants, aux dimensionnements près des équipements. D'une part, le diffuseur de messagerie EMM est unique à chaque site et dispose de sa propre sécurisation (disques miroirs). D'autre part, le signal de sortie de chaque codeur-embrouilleur est analysé par un équipement spécialisé dont les résultats guident le frontal dans sa stratégie de commutation sur le codeur-embrouilleur de secours. Enfin, tous les codeurs-embrouilleurs sont synchronisés par une horloge pilote unique par site.

III. DESCRIPTION DES REALISATIONS.

Matra Communication a développé dans le cadre du projet VISIOPASS un codeur-embrouilleur D2-MAC/Paquet avec contrôle d'accès EUROCRYPT. Ce système de codage-embrouillage est opérationnel et on le retrouvera selon différentes configurations en fonction du site d'émission des informations : point d'émission vers un satellite, point d'émission de réseaux cablés (voir figure 1).

III.1. Environnement technique. (voir figure 2)

Le codeur développé par Matra Communication est l'élément de base d'un système de codage D2-MAC/Paquet, qu'il soit uniquement codeur en clair ou codeur-embrouilleur en accès libre ou en accès contrôlé.

Ce codeur assure le codage et l'embrouillage de l'image, d'un maximum de 8 voies son, l'insertion du télétexte dans le retour trame, la génération des messageries de gestion et de contrôle des titres d'accès. A partir de ces différentes composantes, il est possible de définir un service de télévision, un maximum de 6 services radio, un service d'adressage sur antenne et un service de télétexte.

Le signal D2-MAC/Paquet généré est pleinement conforme aux documents de spécifications D2-MAC/Paquet et EUROCRYPT.

III.2. Structure de base du codeur.

a) Description mécanique.

Le codeur se présente sous la forme d'un chassis 19 pouces de 7 unités de hauteur (dont une de ventilation) prévu pour le montage en baie. Ce chassis supporte l'alimentation,les connexions d'entrées/sorties en face arrière, et, pour la version offrant toutes les fonctionnalités, 19 cartes au format double Europe (6 U de hauteur) de profondeur étendue. Les cartes sont reliées entre elles par un fond de panier qui supporte d'une part un bus VME (P1) et d'autre part des connexions spécifiques (P2).

La réalisation compacte et modulaire a fait appel aux technologies multicouches (jusqu'à 6 couches) et CMS, un grand nombre de fonctions étant réalisées avec des DSP 320C25 et 56000.

b) Interfaces d'entrées. (voir figure 3)

Vidéo :	numérique 4-2-2
Son :	numérique UER/AES 32 KHz ou 48 KHz
EMM :	liaison HDLC 150 Kbits/s
Frontal :	RS232
Télétexte :	liaison HDV bidirectionnelle

Source de synchronisation extérieure (facultative) : horloge, synchronisation ligne, synchronisation trame, compteur de trame

c) Interfaces de sortie.

Signal D2-MAC/Paquet en bande de base, avec ou sans dispersion d'énergie

Signaux de synchronisation

d) Description des cartes

** Gestion du codeur*

- CPU Gérant : cerveau du codeur, il reçoit les paramètres de configuration émis par le frontal via une liaison RS232, et les transmet aux différentes cartes par un bus VME ; la CPU assure également la génération de la ligne 625 ; c'est une carte standard avec un microprocesseur 68000.

** Base de temps*

- BDT : carte base de temps qui génère les différents signaux de service pour l'ensemble du codeur, à partir d'un VCXO qui peut être configuré soit en pilote pour fonctionner en mode autonome, soit être asservi par des signaux de synchronisation extérieurs pour fonctionner en mode asservi ; cette carte génère également les lignes tests CCIR associées aux transmissions.

** Codage MAC*

- SYN : carte synchroniseur, par l'intermédiaire d'une mémoire d'image 4-2-2 ; elle assure la synchronisation du signal 4-2-2 sur l'horloge interne du codeur, horloge dont la précision est celle imposée par la norme D2-MAC/Paquet.

- MAC : cette carte assure les fonctions suivantes : filtrage vertical de la chrominance, compression luminance et chrominance, embrouillage, mise en forme des transitions.

** Génération des paquets son :*

- UER/AES : cette carte assure l'interface entre l'entrée UER/AES et le module de codage son ; chaque carte de ce type réalise l'interface de deux voies UER/AES ; la prise en compte 32 KHz ou 48 KHz est automatique ; cette fonction est réalisée avec un DSP 56000.

- SON : cette carte assure le codage et la mise en paquet d'une voie son stéréo ou de deux voies son mono suivant les deux lois de codage et les deux niveaux de protection, en mode HQ ou MQ ; elle génère également les BI. Elle reçoit tous les paramètres à partir de la carte MPS via une liaison HDV ; cette fonction est assurée par un DSP 56000.

** Génération des paquets de messagerie :*

- CTA : carte contrôleur des titres d'accès, elle génère les mots de contrôle et les paquets ECM à partir de la carte mère PC2 dont elle assure l'interface ; cette fonction est assurée par un microprocesseur 80C51.

- MM : carte multiplexeur de messagerie qui, à partir des informations transmises par le diffuseur de messagerie via une liaison HDLC, met en forme les paquets EMM ; cette fonction est assurée par un DSP 320C25.

** Paquets de la voie d'identification des services :*

- VOIE 0 : cette carte génère les paquets de la voie d'identification des services à partir des informations transmises par la carte CPU ; cette fonction est réalisée par un microprocesseur 80C51.

* *Multiplexage des paquets :*

- MPE : carte multiplexeur paquets entrée ; elle assure le stockage des différentes voies paquets avant leur multiplexage ; chaque carte peut stocker 8 voies paquets.

- MPS : carte multiplexeur paquets sortie ; cerveau du multiplexeur paquets, elle extrait les paquets stockés dans le module MPE pour constituer le multiplex paquets ; cette fonction est réalisée par un DSP 320C25.

* *Embrouillage des paquets :*

- EEB : cette carte assure l'embrouillage d'un maximum de 8 voies paquets à partir des mots de contrôle générés par la carte CTA ; elle supporte 8 fonctions GPA Paquets et la fonction GPA MAC, implantées dans 4 circuits intégrés spécifiques développés par SGS-Thomson ; elle réalise également les fonctions d'entrelacement et de brassage des paquets avec un circuit spécifique développé par SOREP ; cette fonction est réalisée par un microprocesseur 80C51.

* *Multiplexage TDM :*

- TDM : les fonctions réalisées par cette carte sont les suivantes :
  . Multiplexage des données : voies paquets, ligne 625, télétexte, partie données des lignes tests.
  . Codage duobinaire.
  . Constitution du multiplex TDM par multiplexage des données numériques D2, des données numériques 4-2-0 et des données numériques des lignes tests CCIR.

La sortie de cette carte est le multiplex numérique D2-MAC/Paquet sur 8 bits. Cette fonction est réalisée avec un DSP 320C25.

* *Signal de sortie :*

- SOR : cette carte réalise les fonctions suivantes :
  . Conversion numérique/analogique sur 8 bits.
  . Filtrage du signal.
  . Génération du signal de dispersion d'énergie.
  . Circuits de sortie D2-MAC/Paquet et des signaux de synchronisation.

III.3. Configurations.

A partir de ce codeur, divers systèmes de génération du signal D2-MAC/Paquet peuvent être réalisés, le plus simple étant le codeur seul pour générer un signal non embrouillé ou embrouillé en accès libre.

Pour générer un signal D2-MAC/Paquet embrouillé à contrôle d'accès EUROCRYPT, il faut adjoindre au codeur des équipements extérieurs.

a) Configuration 1+0 (figure 4) :

Le système de base est la configuration 1+0 qui comprend un codeur, un diffuseur de messagerie et un PC frontal.

b) Configuration 1+1 (figure 5) :

La configuration 1+1 a été réalisée pour France Télécom à destination de la diffusion par satellite (équipements de Romainville pour TDF1). Elle comporte deux codeurs fonctionnant en parallèle pour le codage d'un canal D2-MAC/Paquet, donc assure une sécurité maximum en cas de défaillance.

Les deux codeurs reçoivent simultanément les signaux suivants :

- Signaux à coder/embrouiller

- Données EMM en provenance du diffuseur de messagerie

- Signaux de synchronisation en provenance du pilote

- Informations de configuration en provenance du frontal

De plus, pour minimiser la perturbation du signal lors d'un basculement d'un codeur sur l'autre, une liaison entre modules CTA permet aux deux codeurs de fonctionner avec les mêmes mots de contrôle.

En cas d'anomalie détectée par un UCDS (Unité de Contrôle des Données et des Sons) en sortie du codeur à l'antenne, une alarme est remontée vers le frontal qui peut prendre la décision de basculer sur l'autre codeur par commande du commutateur de sortie.

c) Configuration N+1 (figure 6)

La configuration N+1 (N<15) est en cours de réalisation pour France Télécom à destination de la diffusion sur les réseaux cablés. A chaque canal est affecté un codeur ; chaque codeur, qui fonctionne indépendamment des autres, reçoit des signaux d'entrée ainsi que des informations de configuration spécifiques au canal.

Un codeur de secours permet de sécuriser le système en cas de panne de l'un des codeurs. La configuration comporte un seul diffuseur et un seul frontal qui gèrent l'ensemble des codeurs. Les signaux de synchronisation issus d'un pilote sont communs à tous les codeurs. Un commutateur aiguille cycliquement la sortie de chaque codeur vers l'entrée d'un UCDS qui assure une remontée d'alarme vers le frontal en cas de panne.

En cas de panne de l'un des codeurs, le Frontal commande l'aiguillage des signaux à coder/embrouiller correspondant vers l'entrée du codeur de secours et la sortie de celui-ci en lieu et place de celle du codeur en panne.

III.4. Bilan de ces réalisations.

S'intégrant dans une gamme complète de produits D2-MAC/Paquet (décodeurs+transcodeurs, outils de tests, générateurs et régénérateurs), cette philosophie de codage permet à Matra Communication d'enregistrer actuellement de bons succès en France et à l'export. Son adaptation au D-MAC est en cours.

IV. CONCLUSION.

Brique importante dans l'architecture du projet VISIOPASS, le point d'émission prend en charge le codage et l'embrouillage des signaux audiovisuels dans un contexte multiopérateurs, multiservices et à accès conditionnel. Selon son affectation, c'est une source de signal D2-MAC/Paquet EUROCRYPT pour un canal satellite ou les canaux d'un réseau cablé.

La présentation des principes définis et retenus par France Télécom pour son architecture a montré que la priorité était donnée dans les deux cas à la fiabilité, à l'identité d'accès pour un opérateur de programme et à l'utilisation d'éléments constitutifs communs aux deux structures. La spécificité satellite ou cable porte sur les modalités de la sécurisation de fonctionnement et sur les divers dimensionnements.

Ces principes d'architecture de point d'émission donnent lieu à des développements industriels en cours, s'appuyant sur la maîtrise technologique de Matra Communication dans le domaine du D2-MAC/Paquet. Les réalisations correspondantes en ont été présentées en détail.

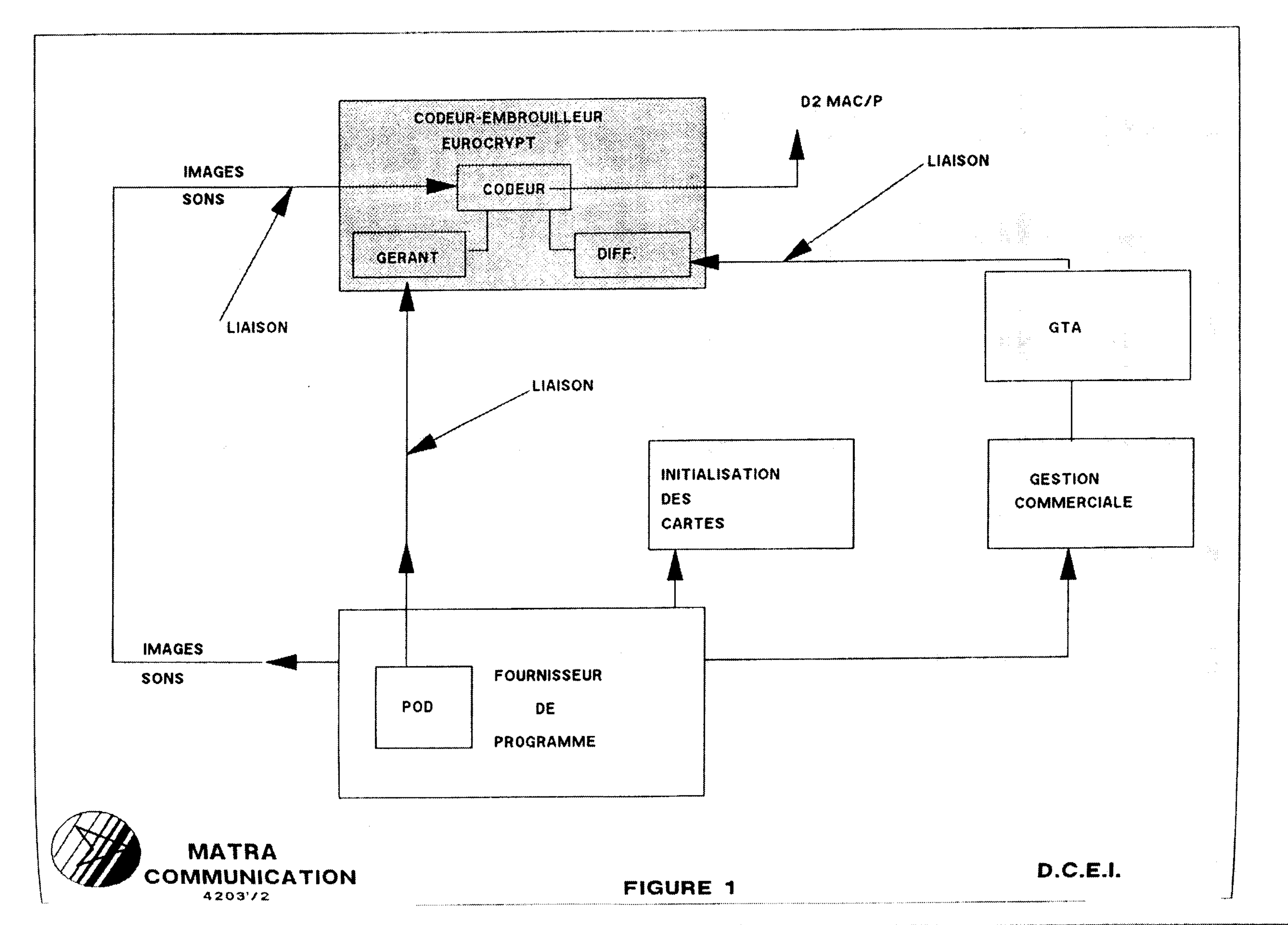

CODEUR-EMBROUILLEUR
EUROCRYPT
CODEUR
GERANT
DIFF.
D2 MAC/P
LIAISON
IMAGES
SONS
LIAISON
LIAISON
GTA
INITIALISATION
DES
CARTES
GESTION
COMMERCIALE
IMAGES
SONS
POD
FOURNISSEUR
DE
PROGRAMME
MATRA
COMMUNICATION
4203'/2
D.C.E.I.

FIGURE 1

FIGURE 2 : CODEUR C2 MAC/P SYNOPTIQUE

INTERFACES D'ENTREES

R
V
B
Sy

CODAGE 4-2-2

4-2-2

SYN (Synchroniseur 4-2-2)

MAC (Codage/embrouillage MAC)

SOURCE DE SYNCHRONISATION EXTERIEURE

Sy/CAFCNT

BDT (Base de temps)

LIGNES TEST

SOURCE SON ANALOGIQUES

CODAGE UER/AES

UER/AES

UER/AES (Interface UER/AES)

SON (Codage son)

SON

MPE (Multiplexeur paquets/entrée)

MPE

MPS (Multiplexeur paquets/sortie)

SEQUENCE D'EMBROUILLAGE MAC

EEB (Embrouillage/entrelacement/brassage)

TDM (Multiplexeur TDM)

SOR (Sortie)

D2 MAC/P

SYNCHRO

EMM

ECM

Mot de contrôle

LIAISON GTA

DIFFUSEUR DE MESSAGERIE

HDLC

MM (Multiplexeur de mess.)

EMMC

CARTE PC2 MERE

CTA (Contrôleur des titres d'accès)

VOIE 0 (Voie d'ident. des services)

BUS VME

FRONTAL

RS232

CPU GERANT

L625

TX

VIDEO COMPOSITE

PONT DE DONNEES

HDV

FIGURE 3 : CONFIGURATION 1+0

SIGNAUX A CODER/EMBROUILLER

DISQUETTE FICHIERS
EMM

LIAISON
GTA
(X25)

DIFFUSEUR DE

MESSAGERIE

DONNEES
EMM

CODEUR

SIGNAL

D2 MAC/P

OPERATEUR

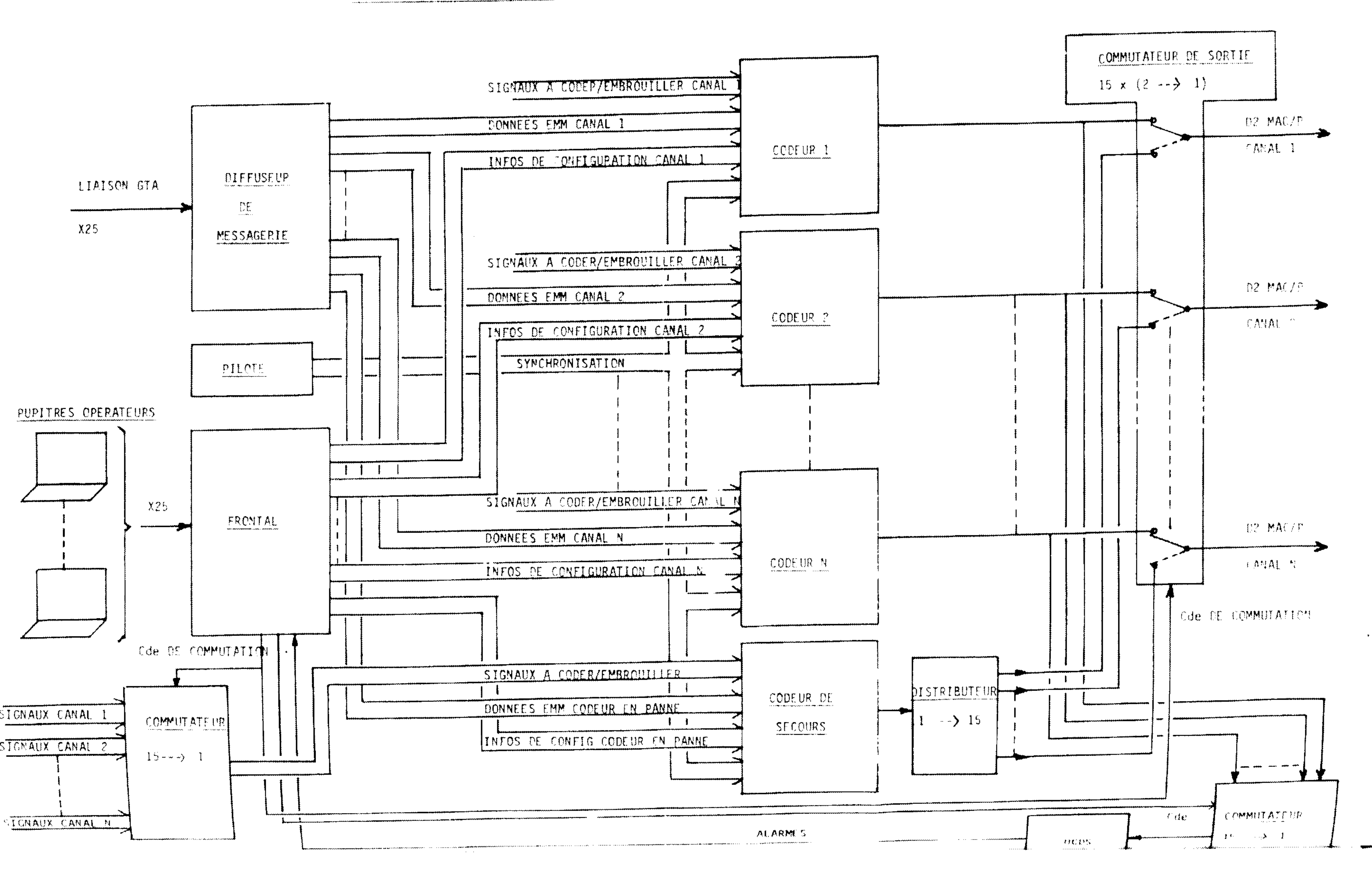
PC FRONTAL

INFOS DE
CONFIGURATION

RS232

FIGURE 4 : CONFIGURATION 1+1

FIGURE 5 : CONFIGURATION N+1



VERSATILE MAC/PACKET ENCODER

INTERFACING WITH

ANY CONDITIONAL ACCESS SYSTEM

Caleb **BRADLEY**, Helge **STEPHANSEN**
Tandberg Telecom a.s.
Box 333
1473 Skårer
NORWAY
Tél : +47 2 973170

ABSTRACT

The MAC/packet coding specified by the EBU in 1984 provides a standard for broadcasting vision, sound and data together in a single channel. The standard has a large degree of flexibility to meet varying demands for these services in the coming decades. In the cases of sound and data services this flexibility is achieved by packet transmission where each packet of digital data contains an address to identify the service it provides. There is provision for scrambling the vision, sound and/or data services, where security can be protected by a chosen Conditional Access System which administrates selective entitlement of receivers, subscriptions, etc. The Tandberg TT12000 Encoder meets these requirements with a configurable architecture which has interfaces both for conventional TV broadcasting and for new services.

RÉSUMÉ

Le codage MAC/paquet spécifié par EBU en 1984 établit un standard de transmission pour vision, son et données dans un seul canal. Le standard est très flexible de façon qu'il est adaptable au besoins variés de ces fonctions dans les dizaines d'années prochaines. En ce qui concerne le son et les données, cette flexibilité est fournie par lemode de transmission paquet où chaque paquet des données digital contient une adresse qui identifie sa fonction. Il y a des possibilités de brouiller les signaux de vision, son et/ou données, où la sécurité est protégée par un système choisi d'accès conditionnel qui gouverne la sélection exclusive des récepteurs, les abonnés... Le Tandberg TT12000 Encodeur remplit ces conditions avec sa construction flexible qui fournit les interfaces aussi bien pour la transmission TV conventionnelle que pour les fonctions nouvelles.

TABLE OF CONTENTS

VERSATILE MAC/PACKET ENCODER INTERFACING WITH ANY CONDITIONAL ACCESS SYSTEM

Caleb Bradley & Helge Stephansen, Tandberg Telecom a.s., Skårer, Norway
Tel. +47 2 97 31 70

1. Introduction

The MAC/packet coding specified [1] by the EBU in 1984 provides a standard for transmitting vision, sound and data together in a single channel of a satellite or a cable network. As was intended, the emphasis today is on use of MAC for delivery of new tv services in the 11.7 to 12.5GHz satellite band, with imminent extensions to stereo and/or multilingual sound and widescreen format. At the same time an evolution proceeds in the exploitation of the multi-purpose packet data channel which is a "free" resource in the coded MAC signal.

The extra packet capacity is a potential source of revenue to broadcasters who have options for its use such as:

- adding sound services
- renting data capacity to third parties requiring one-way wide-area data distribution
- sending encrypted messages which enable selected receiver decoders to descramble transmissions. The arrangement for this is called a Conditional Access System.

The Tandberg TT12000 Encoder has been designed to meet these evolving requirements with a configurable architecture which has interfaces both for tv broadcasting and for the new packet services.

2. Summary of the MAC/packet Multiplex

MAC tv signals retain the scanning frequencies of the terrestrial 625-line standard i.e. horizontal 15625 lines/second, vertical 50 fields/second, 2:1 interlaced. Thus decoders can be built without field storage memory.

Allocation of time within the 625-line frame for MAC/packet is very different from conventional PAL-625 as shown in Fig. 1. The broadcaster is free to choose different time-windows from the usual case shown on the right of Fig. 1 since the "other data" includes information to the decoder about where it will find the rectangular window for each service provided. Thus it is feasible outside tv programming hours to devote all the video part of the frame to extra packet data capacity.

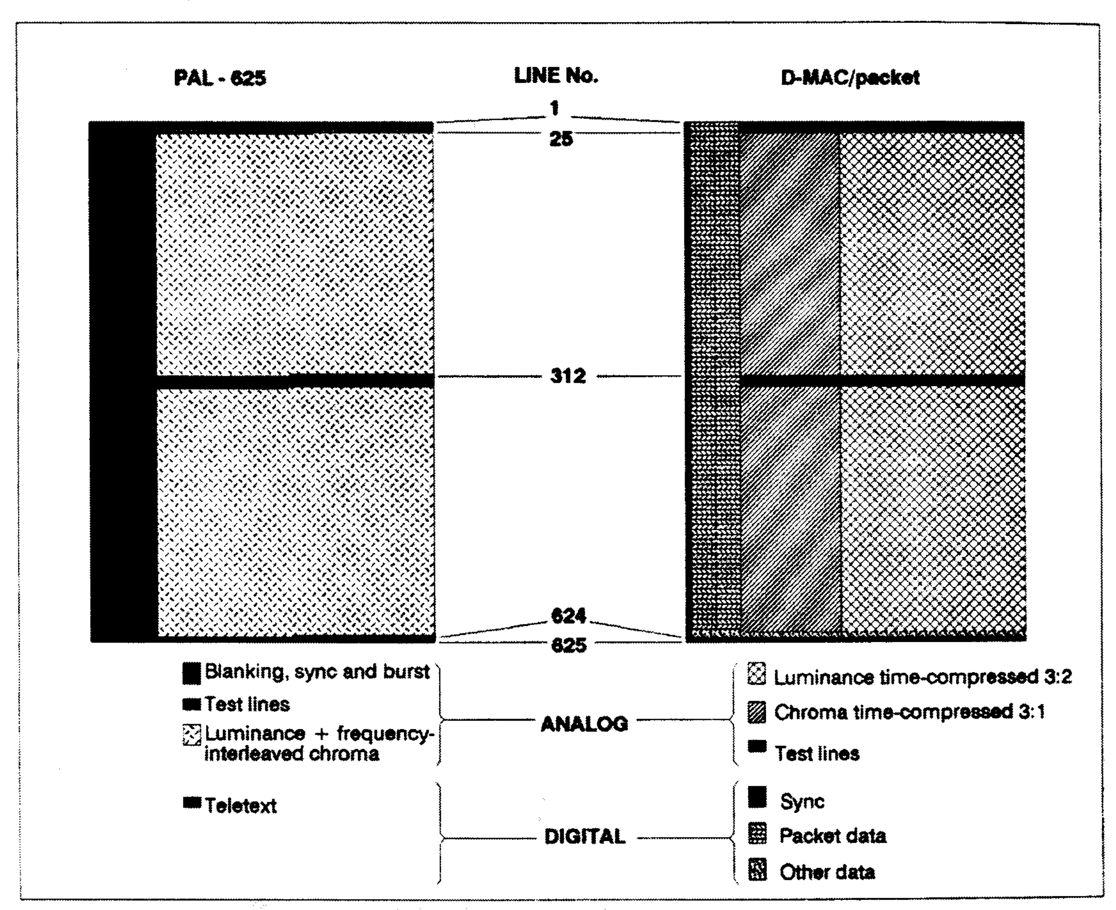


Fig. 1 Comparison of frame partitioning in conventional PAL-625 and D-MAC/packet.

The vision, sound and data components are described below.

2.1 Vision

The chrominance and luminance components of each line are transmitted separately in succession. Thus the well-known imperfections of NTSC, SECAM and PAL coded pictures which arise from imperfect separation of these components are absent in MAC, although the advantage is lost if the decoded signal has to be recoded for conventional receivers without a component-video interface.

Since both components are initially 52μsec long, they both have to be *time-compressed* to fit into their allocated parts of the line. Time-compression shortens the component but causes it to occupy a proportionally wider frequency bandwidth. Luminance with the wider initial bandwidth of about 5.5MHz is time-compressed by a lesser ratio (3:2)

than chrominance (3:1) so that both after compression occupy about 8.25MHz. The channel bandwidth constraint of terrestrial broadcasting does not apply here.

2.2 Sound

Sound is transmitted digitally in MAC. The broadcaster can choose between several options such as:

- High quality 15kHz or Medium quality 7kHz bandwidths
- Linear 14-bit or NICAM* coding
- Stereo or monophonic
- Simple ("1st level") or more robust ("2nd level", Hamming code) protection against bit errors

*NICAM = Near-Instantaneous Companded coding in which sound samples are transmitted with 10-bit resolution, with groups of 32 samples scaled by a factor which is signalled in the sample parity bits.

In all cases the digital sound data is collected into packets, called BC, which are transmitted as described below. The rate at which BC packets are sent depends on the above options but will seldom exhaust the available capacity, even with as many as 8 high-quality sound channels. Periodically a packet type called BI is also transmitted to tell the decoder which of the sound options is in use.

2.3 Packet Data

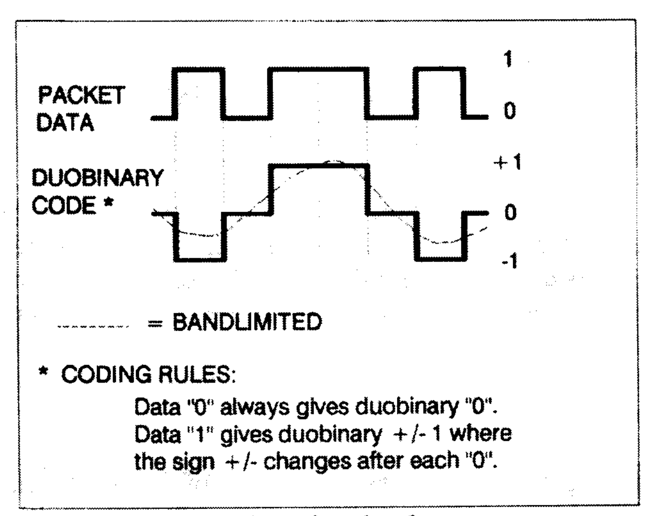


Fig. 2 Duobinary coding of packet data.

Packet data is transmitted in a 9.8μsec burst on each MAC line except 624 and 625 as shown in Fig. 1. The binary data bits are sent in the form of a three-level (+ 1, 0, -1) or duobinary code, see Fig. 2, which can be band-limited to suit the channel.

The variants D-MAC and D2-MAC differ in data rate, and thus in the channel bandwidth required, as follows.

Standard	*Data rate*	*Packet bits per line*	*Base bandwidth*	*Intended uses*
D-MAC	20.25Mbit/sec	2 x 99	8.4MHz approx.	FM in satellite 27MHz channel, AM in cable 12MHz channel
D2-MAC	10.125Mbit/sec	99	< 5 MHz	FM in satellite 27MHz channel, AM in cable 8 or 12MHz channel

In D-MAC the data period is divided into two successive 99-bit bursts, shown by the dashed line in Fig. 1, which are used for independent packet streams. This allows control of which packet services are retained if a D-MAC signal has to be recoded as D2-MAC.

Several types of packets may be sent:

- Sound BC and BI packets - see above
- SI (Service Identification) packets - contain information on all services carried on the signal, additional to the short SI information in line 625
- General data packets - identified by their addresses
- Teletext packets
- Packets for Conditional Access management.

More details of packet processing (prioritising, scrambling, interleaving) and Conditional Access are given below.

3. Scrambling

Scrambling may be applied to any service to restrict its reception, but not to basic information needed by all receivers such as sync., lines 624 and 625, and headers of packets. Scrambling is done using pseudorandom bit-sequences which can be generated by shift registers connected with appropriate feedback. The structure of these registers is not secret; it is available to anyone in [1] and they are built into every MAC decoder because the decoder to succeed in descrambling a service has to duplicate the sequence used in the encoder.

Security of scrambling is given by the extreme length of the pseudorandom sequence. A 60-bit *control word* is used at the encoder to start ("seed") the sequence at some point. Authorised receivers are given the same control word in a controlled manner and so can seed their sequence identically, while would-be pirates have a practically impossible task of finding the seed where there are astronomically many possibilities.

Further security is given by camouflaging the pseudorandom sequence with a 256-frame count, and changing the control word every 10.24 seconds. Different services can use different sequence generators with different control words.

An *encryption* system external to the encoder is needed to convey the secret control words exclusively to the decoder(s) authorised for (subscribing to) each service, see Conditional Access below.

The mechanisms of scrambling video and data/sound which are implemented in the TT12000 Encoder are described below.

3.1 Vision Scrambling

Two methods of cut-and-rotate are available:

- Single-cut in chroma and rotate line
- Double-cut (in luminance and chroma) and rotate within each component.

In either method, each cut is made at a pseudorandomly-chosen one of 256 possible cutting points in luminance or chroma. The result on one line is shown in Fig. 3. Since the cut point(s) are chosen by a scramble sequence generator and differ from line to line, the picture becomes unrecognizeable. All transitions between unrelated compo-

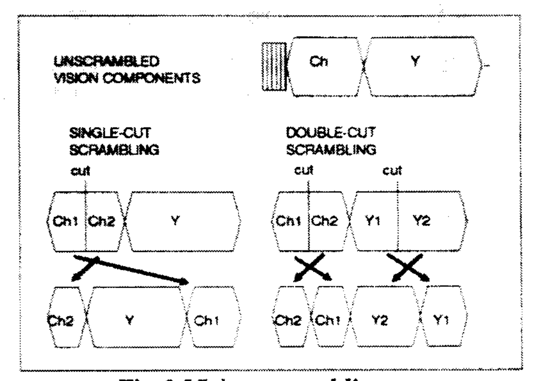


Fig. 3 Vision scrambling.

nents are smoothed by cross-fading to avoid artifacts which could ease pirate descrambling.

The same cut-and-rotate process is used in decoders to recover the picture.

3.2 Packet Data Scrambling

The information part (not the header) of any packet service including sound packets may be scrambled. Scrambling is done by adding modulo-2 in an EXclusive-OR gate the serial packet data to a pseudorandom sequence from a scramble generator. The

decoder recovers the information from the scrambled stream by the same process using the same sequence.

In addition all packet data is interleaved, see 5.3.2 below, and randomised to spread its frequency spectrum to reduce interference to nearby channels. Interleaving and randomising are reversed in the decoder.

4. Modulation

The baseband D- or D2-MAC signal as described may be processed as follows for satellite broadcasting.

- *Pre-emphasis* as is normal prior to frequency modulation, to improve overall signal-to-noise ratio.
- *Dispersal* is addition of a frame-rate (25Hz) triangle wave intended to spread the frequency spectrum.
- *Frequency modulation* of 70MHz intermediate frequency (i.f.)
- *Limiting* to remove residual amplitude modulation of the i.f.
- Harmonic filtering
- Conversion to uplink frequency

For cable systems the MAC/packet signal may be amplitude modulated with vestigial sideband filtering and distributed in a channel bandwidth of 12MHz for D-MAC, or about 8MHz for D2-MAC.

5. Encoder Architecture

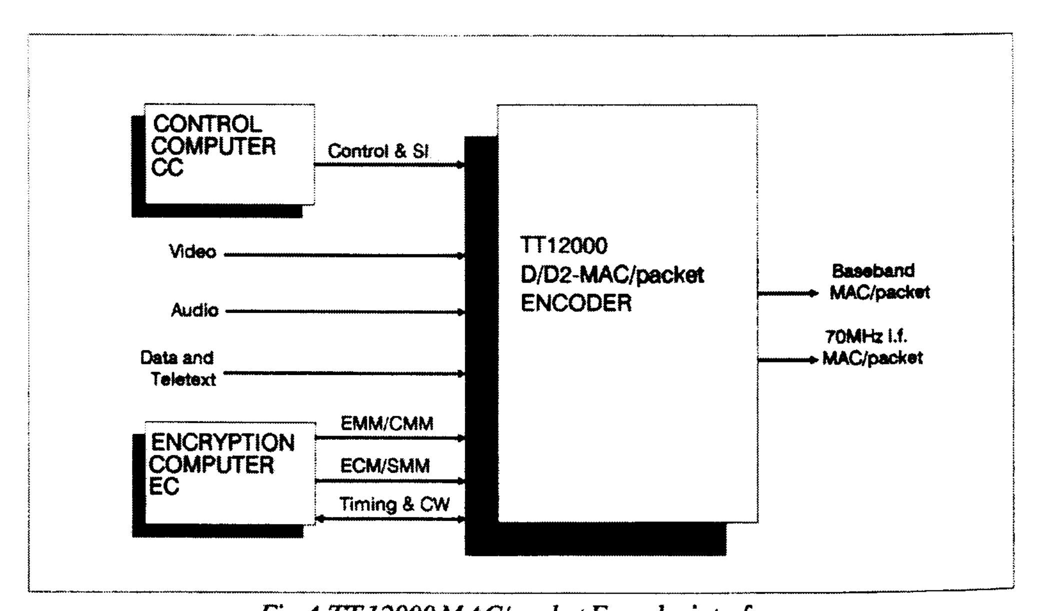


Fig. 4 TT 12000 MAC/packet Encoder interfaces.

External interfaces to a MAC/packet Encoder are shown in Fig. 4. Processing of the vision, sound and data inputs is described below. Two computers shown in Fig. 4 are used to configure the Encoder for the services required (and generate the SI infor-

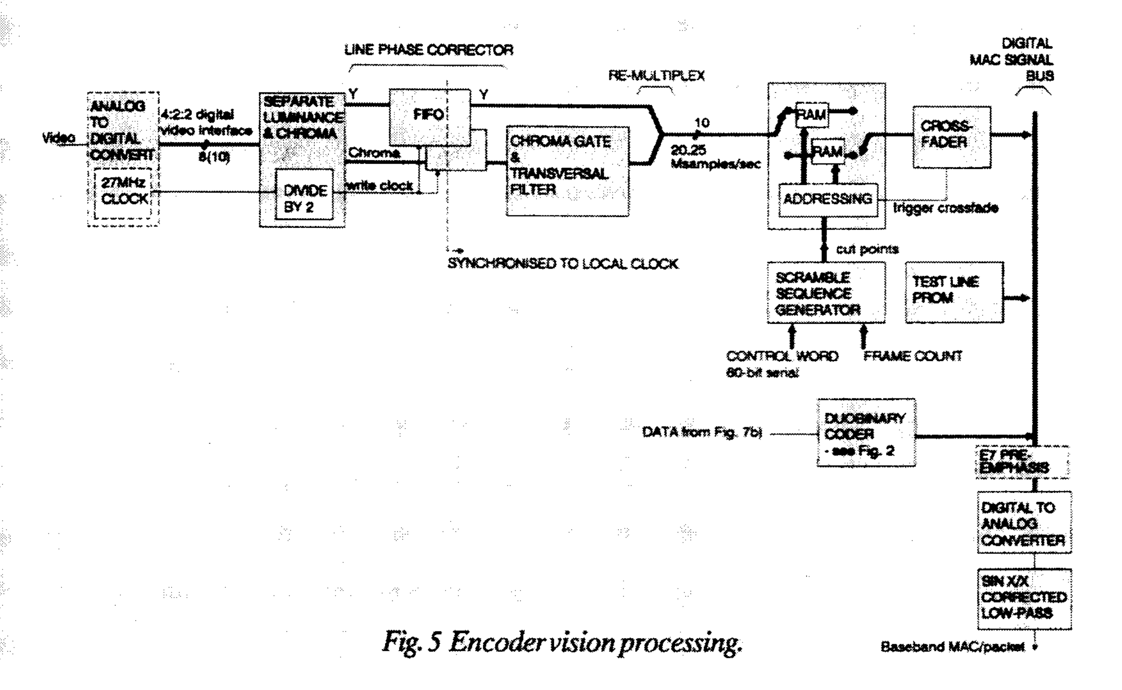


Fig. 5 Encoder vision processing.

mation carried on the MAC signal), and to generate control words and messages for a Conditional Access system of encryption.

5.1 Vision Processing

The vision processing chain is shown in Fig. 5. The processing is digital, with analog video input via an optional converter if standard 4:2:2 digital video [2] is not already available.

Incoming digital video consists of parallel 8-bit samples (the encoder can accept 10-bit samples) with accompanying sample clock 27MHz. Luminance and chroma samples are first separated into two 13.5Msample/sec streams which are written into FIFOs (First In, First Out memories). These serve as "elastic" delays which absorb line phase difference so that all subsequent processing can be phased to the local clock source. This may be free-running or be locked to an external reference, not shown.

The FIFO for chroma passes alternate samples of each colour-difference component. In the following stage, alternate colour-difference components are gated out on each line, since there is room for only one component of chroma on the MAC line. This gating has two consequences:

- When chroma is again multiplexed with luminance the total rate is reduced from 27 to 20.25Msamples/sec,

- transversal filtering of chroma is needed to reduce aliasing of high vertical spatial frequencies.

Normally a 3-line transversal filter is used. The Tandberg TT12000 Encoder employs a 7-line filter with coefficients optimised for better transient response. Such a filter needs to be able to adapt towards the top and bottom of the picture to implement 5-line, 3-line and 1-line (no filter) weightings.

The stage "Compression Memory" contains two RAMs (Random Access Memories) which alternate on successive lines between writing and reading. Several functions are achieved merely by control of address counters for the RAMs:

- Luminance and chroma are read out separately at the correct times on the MAC line. The readout rate is 20.25Msample/sec in each case, which gives the time-compression factors 3:2 and 3:1 respectively.
- Luminance is delayed by 3 lines relative to chroma, using a 3-line rotating buffer in the RAM. This over-compensates the delay to chroma in the transversal filter, resulting in chroma being transmitted a line ahead of luminance. The MAC standard [1] arranges this to minimise the amount of memory required in receivers to implement a 3-line transversal filter to interpolate the missing lines of colour-difference information.
- The vision components are scrambled as shown in Fig. 3 by loading the reading RAM address counter with cut-point data from a pseudorandom scramble sequence generator.

The Cross Fader smooths transitions between unrelated components by synthesizing three samples in the transition region. The Compression Memory provides a trigger pulse to initiate a crossfade whenever the reading address count is interrupted, e.g. at scrambling cut-points.

The signal multiplex in Fig. 1 is completed in digital form when optional lines of test video from a PROM, and data which has been duobinary coded and band-limited as shown in Fig. 2, are combined on a bus. The optional digital "E7" pre-emphasis module shown in Fig. 5 uses non-linear processing to achieve 2-4 dB better overall signal-to-noise ratio than conventional linear pre-emphasis. The composite MAC/packet signal is finally converted to the baseband analog output.

Several video processing functions in Fig. 5 allow modification by the Control Computer. The options include chroma filter on/off, clipping of chroma, choice of no scrambling or single-cut or double-cut, forcing "free access" scrambling i.e. scrambling with a fixed non-secret control word, and inserting at the FIFO outputs test lines or pictures stored in PROMs (not shown).

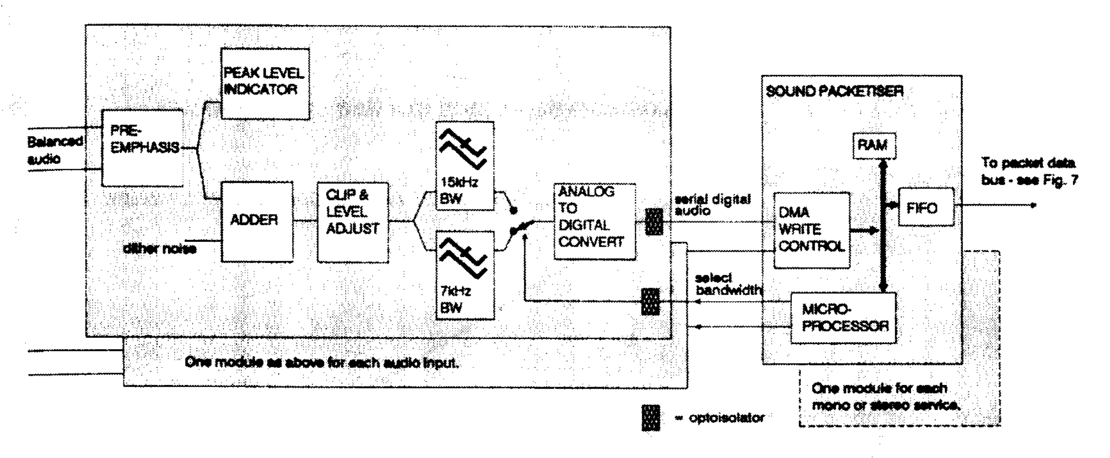


Fig. 6 Encoder sound processing.

5.2 Sound Processing

The Sound Processing is shown in Fig. 6. The analog circuits are in identical modules, one for each audio input, which are contained in their own frame and interface with the rest of the encoder via optoisolators to prevent crosstalk from digital circuits.

Each balanced audio input is pre-emphasised [3] and a dither noise is added. This reduces the subjective effect of the subsequent 14-bit quantising. Before quantising, the signal must be low-pass filtered to prevent aliasing. Alternative filters are selected by an electronic switch for high-quality or medium quality service.

The analog-to-digital converter gives a serial data output which is written into RAM in a Sound Packetiser module by d.m.a. (direct memory access). The microprocessor in this module "knows" which of the options in 2.2 above to implement and is able to create BC (sound data) packets, and periodic BI packets. It writes the packets to an output FIFO which interfaces with the packet data bus similarly to all other packet generators, described below.

5.3 Packet Processing

The packet processing shown in Figs. 7a) and b) is the most complex part of the encoder. Up to 24 packet generators may be fitted of various types, including sound packetisers, depending on the input interfaces required. These may be a high-speed parallel interface, a slower RS232 serial interface, and/or an X.25 LAPB [4] packet network interface.

All packet generator modules are set up by the Control Computer which delivers, via a Buffer Processor and a multiprocessor Serial Control Bus which visits each module, configuration data for each service which includes:

- Packet address(es) to appear in headers
- Packet type e.g. BC, BI, EMM, ECM (see below), etc. (appears in header)
- Packet rate or maximum period between packets

- SI content (packetised in a dedicated module)

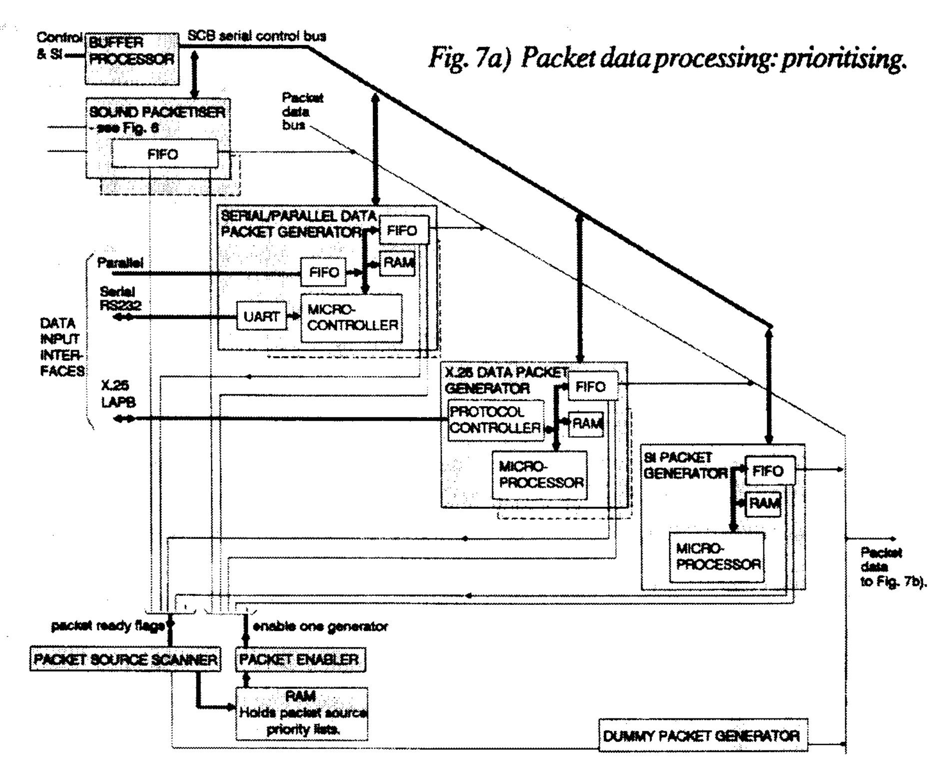


Fig. 7a) Packet data processing: prioritising.

The SCB is also used by the computer to load lists of service parameters into the RAMs shown in Figs. 7a) and b), and to configure the vision and sound processing. Tandberg provide an easy menu-driven user interface for setting up vision, sound and data services with the program *ENCON* which runs on an IBM-compatible PC.

There are two stages of buffering for all packets, associated with *prioritising* and *interleaving*.

5.3.1 Packet Prioritising

All packet generators compete to deliver their packets to the packet data bus. The packet prioritiser arbitrates by scanning to find which generator(s) have packets ready in their output FIFOs, and enables one generator at a time to drive the packet data bus. The priority rules are held in a RAM and are usually chosen to be as follows:

- Sound packets have top priority - they must not be delayed by data because of limited buffering in decoders.
- SI packets have medium priority - the rate of SI packets affects the time for decoders to acquire a service

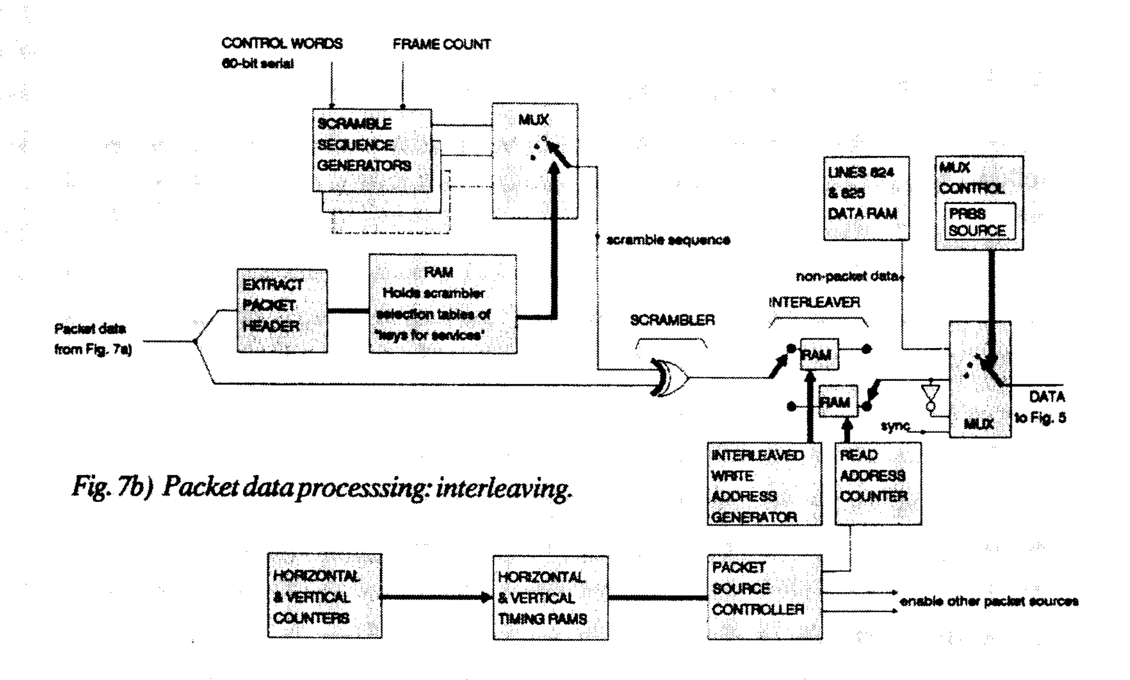


Fig. 7b) Packet dataprocesssing: interleaving.

- Data packet services have relative priorities according to requirements.
- "Dummy" packets have lowest priority and are generated automatically to fill unused capacity in the MAC sub-frame.

The enabled generator delivers its packet to the Scrambler. The address in the header of the packet is extracted and used to select, via a table in RAM, the pseudorandom scramble sequence generator for that service, which has already been seeded with the correct Control Word.

5.3.2 Packet Interleaving

The output of the EXclusive-OR scrambler gate is written to one of two alternating RAMs. The address generator for this RAM gives an interleaved sequence so that when the packet is read out again with a simple incrementing address sequence, the order of bits is changed. If the original packet bits are numbered 1, 2, 3,.... 751 the bits transmitted are 1, 95, 189,..... i.e. step size = 94 bits.

Transmitting the 751 bits in this non-sequential order is intended to improve resistance to burst errors by distributing the vital 31-bit header.

5.3.3 Packet Time Multiplexing

Insertion of packet data in the MAC line in bursts at correct time(s) is achieved as follows. The plan of frame multiplexing, which is defined by the SI and may be that shown in Fig. 1, is loaded into Horizontal and Vertical Timing RAMs. These are addressed by horizontal and vertical counters synchronised to the frame.

At the time(s) in the line of a data sub-frame(s) the Packet Source Controller enables readout from the Interleaver of a burst of 99 bits. The Packet Source Controller has expansion possibility for multiple data sub-frames and other data sources, e.g. Teletext, which are not shown in Fig. 7b).

The output multiplexer in Fig. 7b) combines packets with other non-packet data such as sync data, and lines 624 and 625. It randomises the packet data by selecting between direct and inverted bits under control of a local pseudorandom source.

6. Conditional Access

The Encoder performs scrambling, using control words (keys) and a table of keys-for-services which is loaded via the Buffer Processor in Fig. 7a). The Encoder also provides, as part of the packet capacity, a channel for sending cryptograms to the decoders.

Conditional Access systems use both these facilities of the Encoder to selectively enable decoders to descramble particular services. The types of cryptogram which may be sent are:

- ECM Entitlement Checking Message - contains the control word for a service (or group of services) encrypted by, and only decryptable using, an authorisation key.
- EMM Entitlement Management Message - contains the authorisation key for decrypting the above encrypted by, and only decryptable using, a distribution key which is restricted by physical means to authorised user(s).

The TT12000 Encoder is able to interface with any of the three Conditional Access systems below which are registered with the EBU.

6.1 Eurocrypt M

This Conditional Access system is developed and proposed by CCETT (France). The control words and ECM are generated in the encoder by a special module which carries a "smart" plastic card reader and fits into the packet generator section in Fig. 7a). The EMM content can be downloaded from an off-site customer administration

centre over an X.25 packet data network to an EMM injector. The EMM injector then transmits EMM packets with the required priority and rate.

6.2 Eurocrypt S

This system is proposed by the Norwegian Telecommunication Administration (NTA) in cooperation with NR/MSK representing the nordic telecommunication administrations and broadcasting organisations.

Instead of ECM/EMM the packets sent are:

- SMM Service Management Message, similar to ECM.
- CMM Customer Management Message, similar to EMM.

CMMs can be used alone to give static subscriptions, while CMMs and SMMs together allow dynamic control of subscriptions, such as pay-per-view schemes.

Control words are downloaded to the encoder over a dedicated RS232 interface. The SMM and CMM can be injected by one or two of the parallel or X.25 LAPB data packet generator modules shown in Fig. 7a).

The control computer, CC, sets up the addresses for the SMM/CMM packets. The same addresses have to be used by the encryption computer EC. These may be separate computers at different locations so there is a need to transfer the address table between CC and EC. This can be done by a separate link. An alternative and better way is to configure the control word interface in a dual handshake mode where the addresses for SMM/CMM are sent from the encoder control word port to the EC.

The TT12000 Encoder is in operation with the Eurocrypt-S system transmitting Swedish Television 1 and 2.

6.3 Eurocypher

This Conditional Access system is developed and proposed by General Instruments Inc. Also in Eurocypher the control word (CW) generator and the encryption equipment are separate from the encoder. Packet addresses are transferred between CC and EC by a dedicated link. The CWs and ECM/EMM are downloaded to encoder input ports. The CWs then go to the scramble sequence generators. The headers of ECM/EMM packets are checked before transmission to verify correct packet address and freedom from detectable errors.

The TT12000 Encoder is in operation with Eurocypher on the BSB (British Satellite Broadcasting) channels.

References

[1] *Specification of the Systems of the MAC/packet Family*, EBU Tech. 3258-E, October 1986.

[2] *EBU Parallel Interface for 625-line Video Signals*, EBU Tech. 3246-E, August 1983.

[3] CCITT J.17 Pre-emphasis

[4] CCITT Fascicle VIII.3 - Recommendation X.25 *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for Terminals Operating in the Packet Mode and Connected to Public Data Networks by Dedicated Circuit*, 1984

THE NORDIC VLSI MULTI MAC CHIP SET

FOR CONDITIONAL ACCESS CONSUMER RECEIVERS

Leif Arne **RONNINGEN**
Nordic VLSI
Øvre Flatåsvei 4D
7079 FLATASEN
NORWAY
Tél : +47 7 98 62 11

TABLE OF CONTENTS

1. Introduction

The advantages of the MAC system are well known. MAC offers much better picture and sound quality than existing systems, as well as service access control, and digital data transfer services. The system permits the capacity of the time division multiplex to be used in a very flexible way:

- Picture with a number of sound channels plus data channels
- Sound and data channels (20 Mbits/sec)
- Data channels, full-field (20 Mbits/sec)

Further, the MAC system is compatible with HDMAC, the coming system for HDTV in Europe.

2. The Nordic/Philips/Plessey MAC chipset

The design of the multi MAC chipset (NPP chipset) was initiated by The Norwegian Telecommunications Administration (NTA) in 1985. A few months later Nordic presented a decoder and chip architecture, based on the following philosophy:

- Complete multi-MAC implementation
- Conditional access from day one
- Utilization of the multiplex flexibility
- Low cost minimum solution for low-end consumer receivers
- Extendable to more sophisticated consumer receivers and professional receivers

The chipset has been used in professional MAC receivers since summer '89, and volume production for consumer receivers is in progress at Philips Components and Plessey Semiconductors.

The chipset consists of some basic building blocks as shown in figure 1.

The analog MACAN chip provides gain control and clamping of the video signal, data demodulation, and clock recovery.

The CONTROL chip can be programmed to receive all possible TDM multiplex configurations, and to control synchronization, packet acquisition, filtering and buffering, error correction, and timing. A serial PACKET BUS outputs all packets from two data bursts, which can be configured to cover the D and D2 MAC standard double and single bursts, or two data burst covering full-field data (20 Mbits/sec).

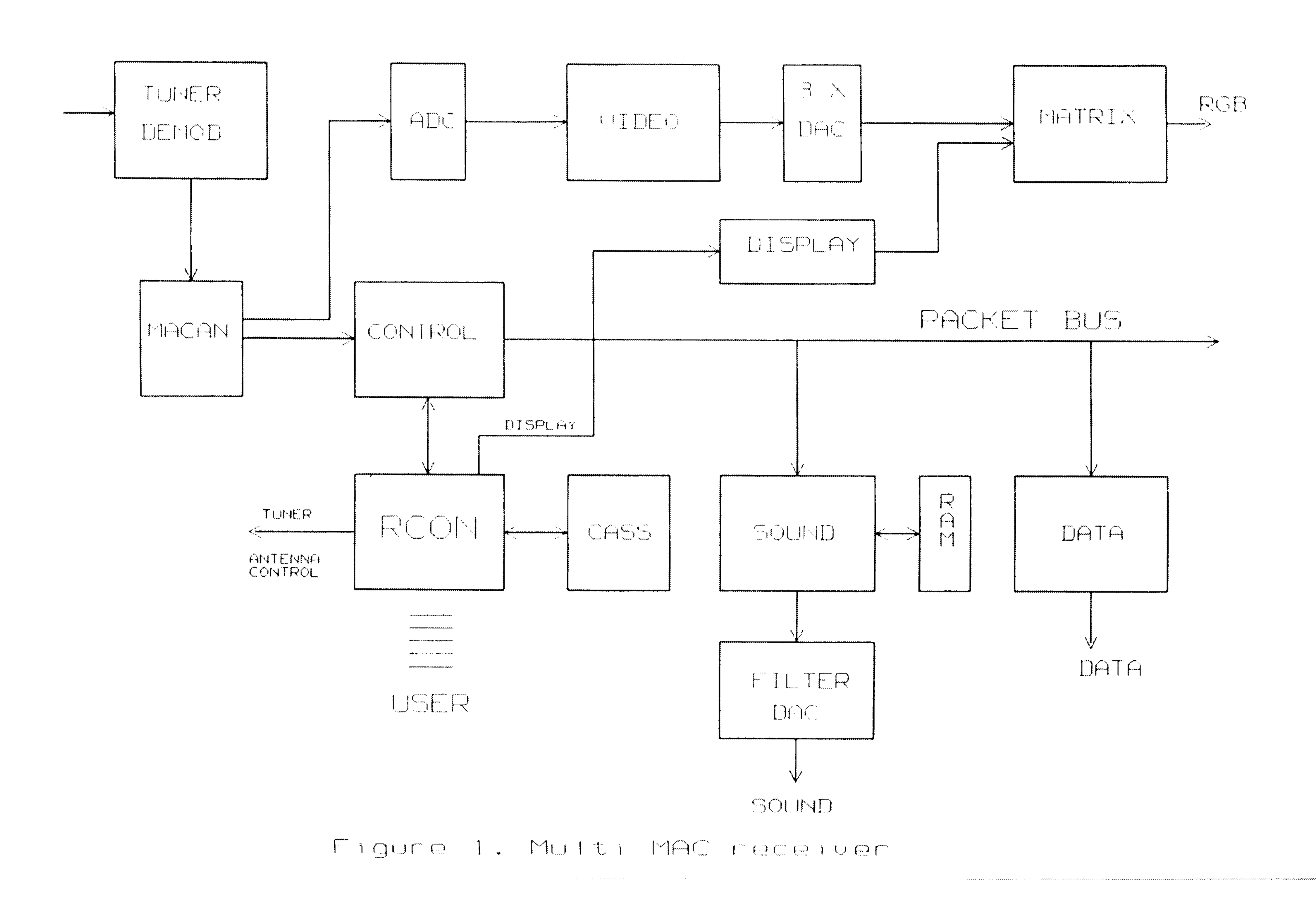


Figure 1. Multi MAC receiver

Packets concerning conditional access and service identification (SI), and line 625 are filtered, error corrected, and buffered. A very fast parallel interface (> 2 Mbytes/sec) transfers these packets to the receiver control. A standard cheap microprocessor can read all packets from one 99 bits data burst without packet loss. This means that only one packet buffer is needed in the CONTROL chip.

RCON (Receiver Control) can be implemented with one or more processors and software. RCON controls the programmable chipset in a simple and efficient way by means of the CONFIGURATION CHAIN feature. This is effectively a long shift register running through all chips, loaded via the CONTROL chip.

RCON configures the CONTROL chip to sort out wanted decryption packets, and conveys them to CASS. The protocol towards CASS, covers both variants of the EUROCRYPT standard, and is based upon the ISO 7816 smart-card standard.

RCON sorts out and processes the data received from line 625 and SI packets, and structures and stores the information.

RCON also handles the user interface.

The CASS (Conditional Access SubSystem) handles the decryption packets received from the CONTROL chip via RCON, and returns control words for descrambling if the actual services are ordered and paid for.

The VIDEO chip handles the 4:3 and 16:9 aspect ratios and panning. The on-chip descrambler receives control words from CASS via RCON, the CONTROL chip and the CONFIGURATION CHAIN.

The SOUND chip implements the complete MAC specification, and decodes two encrypted sound services. Mixing of sound is controlled in a very flexible way from RCON via the CONFIGURATION CHAIN. BI packets are processed on-chip.

The on-chip descramblers receive control words from the CONFIGURATION CHAIN.

The sound chain architecture supports decoding of up to 48 encrypted sound services in an economical way, simply by connecting a number of SOUND chips in parallel to the PACKET BUS.

The DATA chip extends the data transfer capability of the NPP chipset. With its packet acquisition modules, descramblers, teletext transcoder, and packet buffers, it is outstanding for encrypted data transfer; for data rates from kbits/sec to 20 Mbits/sec. The buffers can be read via a standard parallel microprocessor bus. If required, a number of DATA chips can be connected to the PACKET BUS.

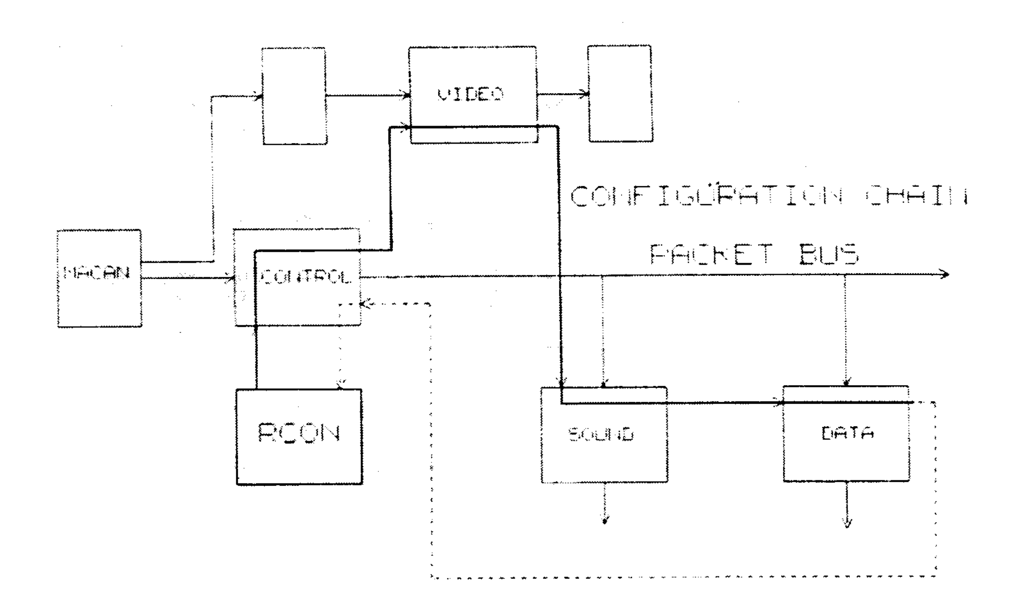


Figure 3. The Configuration chain

3. Receiver control and service access control

As described in chapter 2, RCON controls the MAC decoder. In addition, RCON controls the CASS, the antenna, and the tuner, and provides an interface towards the user.

Although the NPP chipset can be used together with several conditional access standards, the description here is based on EUROCRYPT S and EUROCRYPT M.

The MAC/EUROCRYPT systems are very flexible, and offer the user a large number of possible combinations of services and access modes. To handle this, a sophisticated but user-friendly man-machine interface is necessary. People have different background and skills in using technical equipment. The man-machine interface should support both the user that wants access to a basic service by just pushing a button, and the advanced user that wants to utilize all possibilities.

An important aspect is compatibility with existing TV sets. This implies that when the acquisition of a service proceeds rapidly in a normal manner, no information should be given to the user until the picture and sound appears. But it is very important to inform the user when access to a service, for one reason or other, is delayed or not permitted. The display of this information must be given a form which is interpretable for the man in the street. Text and symbols on the TV screen is probably the best, but other methods, for example by means of LEDs, should be considered.

A substantial portion of TV sets manufactured the last ten years have infrared remote control. Many TVs also have teletext facilities. It is likely that the users of future MAC TVs want the same features, and then the basis for a user-friendly man-machine system is present.

The EUROCRYPT S standard defines several modes of operation. The most important are:

* Static subscription (no service management message)

* Dynamic subscription

  - Subscription per element, or "a la carte"

    The service provider divides the service into service or programme elements, and offers any combination to the customer.

  - Subscription per tiered element

    The service is divided into components A, B, C, D etc, and the customer can subscribe on alternatives A, A+B, A+B+C, etc.

  - Pre-booked programme number

    Any programme, referenced by a number, can be ordered in advance.

  - Impulse pay-per-view per program

    The customer buys in advance programmes for a certain amount of money, and an "account" in the CASS is credited correspondingly. When the customer uses the facility his account is charged with the price of of the program.

  - Impulse pay-per-view per time unit

    The same as above, but now the customer is charged per time unit.

* Group control

  Groups of customers, grouped geographically or by subject, will replace the service for some time, or receive a text page, or perform fingerprinting.

The SI system (packets with address '0' and line 625) provides information on services and data for acquisition of services.

RCON consists of three main functional blocks, as shown on figure 3.

The CORE contains control functions which are standardized, and could be the same for all receiver models.

The CIF covers the CASS interface protocols for EUROCRYPT S and EUROCRYPT M. This module may be placed on the same physical hardware as CORE.

ASW consists of a number of blocks which are specific to each TV manufacturer and receiver type. This module may be placed on a dedicated processor, or together with CORE.

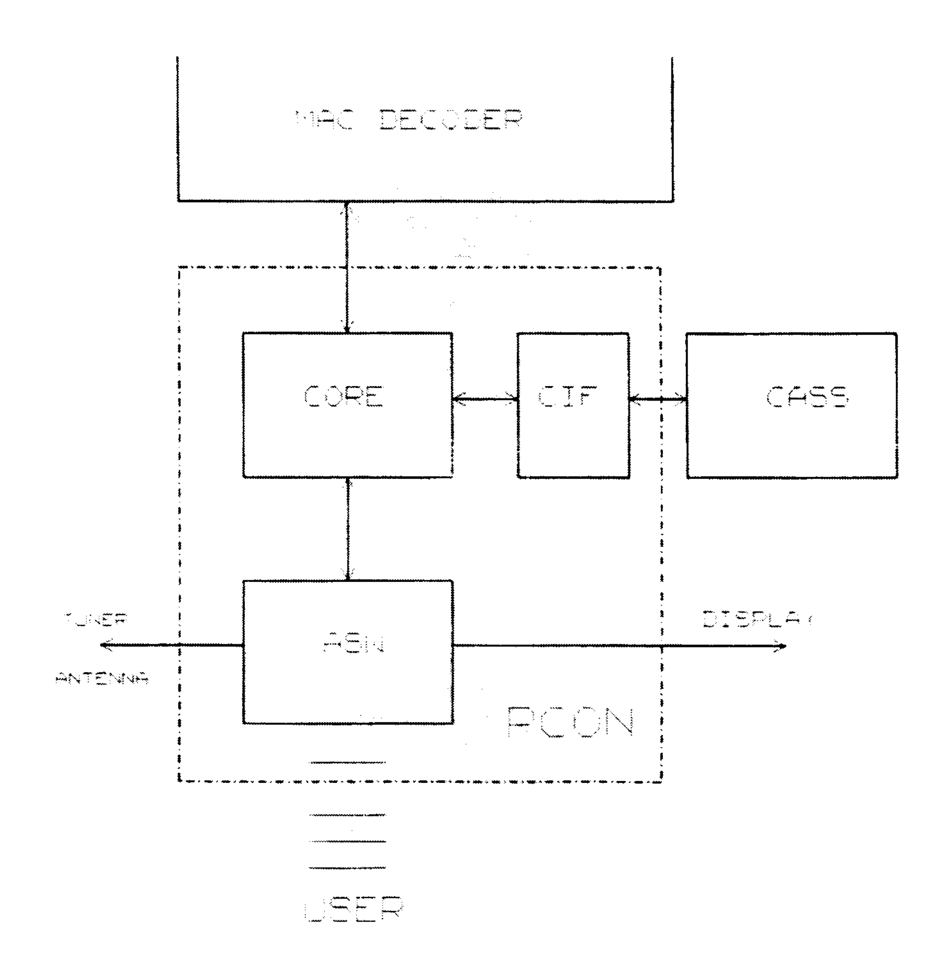


Figure 3. RCON functional blocks

3.1 **CORE** - RCON Core Functions

The CORE communicates with the MAC decoder, CIF and ASW. CORE does not see any difference between the EUROCRYPT S and EUROCRYPT M standards, this is covered by CIF. The interface towards ASW will be the same for all cases.

CORE functional blocks:

- Scheduler
- MAC decoder interface
    - Configuration chain
    - Packet reception
- CIF interface
- ASW interface
- Line 625 handler
- SI handler (pa0)
    - Data group structuring
    - D2 MAC/EUROCRYPT M data group error checking
- CMM handler
    - CMM_EG
    - Other CMMs
- SMM handler
- Sound mix handler
- BER handler
- Data channel handler

3.2 **CIF** - RCON - CASS Interface Module

The CIF module communicates with CORE and one or more CASSes. Both EUROCRYPT S and EUROCRYPT M are covered. The CORE Interface is the same in all cases.

3.3 **ASW** - RCON Application Software

The ASW covers functions which are specific for each receiver model. ASW communicates with CORE, the tuner, the display or teletext system and the user.

ASW functional blocks:

- CORE Interface
- Man-machine Interface
  - Service info and select
  - Conditional access info and select
  - Operational info and select
  - Maintenance
  - Help
- Teletext/display control
- Tuner control
- Antenna control

3.4 Behavioural description of RCON

The signal sequence diagram in figure 4 shows the behaviour of RCON and the environment after power on and change of channel using D-MAC/EUROCRYPT S. It is assumed that entitlements for the service (TV picture + main sound) is stored in the CASS. Group Control is used to replace the service when commercials are shown.

The signal names (commands, parameters) used in figure 4 which are not self-explanatory are defined in the Eurocrypt S specification.

4. Applications

Figures 5 to 8 show several applications of the NPP chipset.

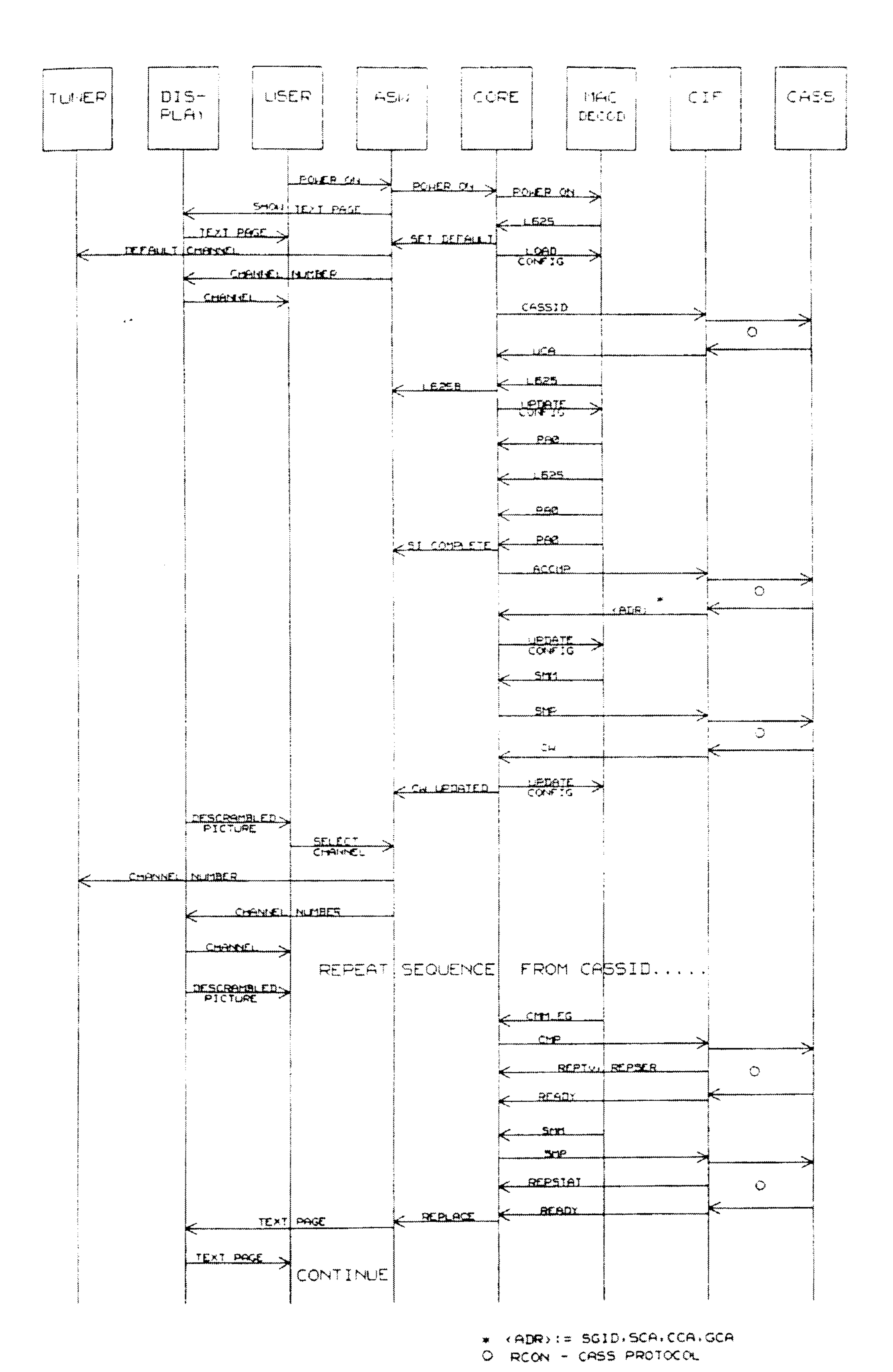


Figure 4. Signal sequence diagram, receiver behaviour.

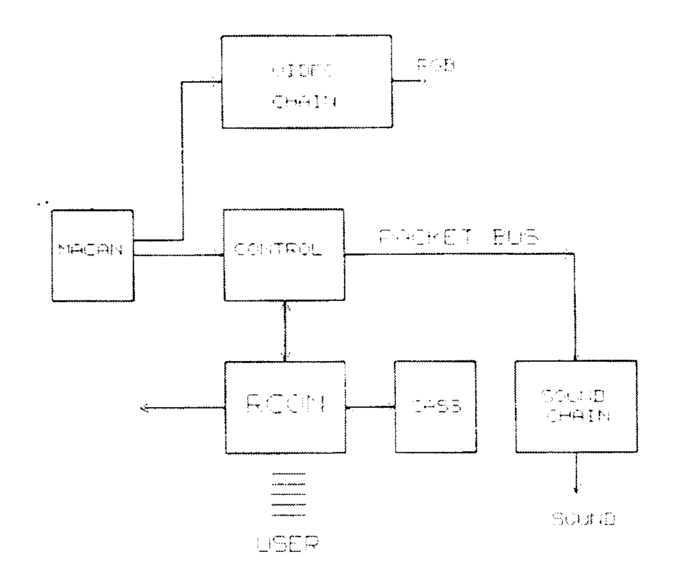


Figure 5. Minimum MAC receiver

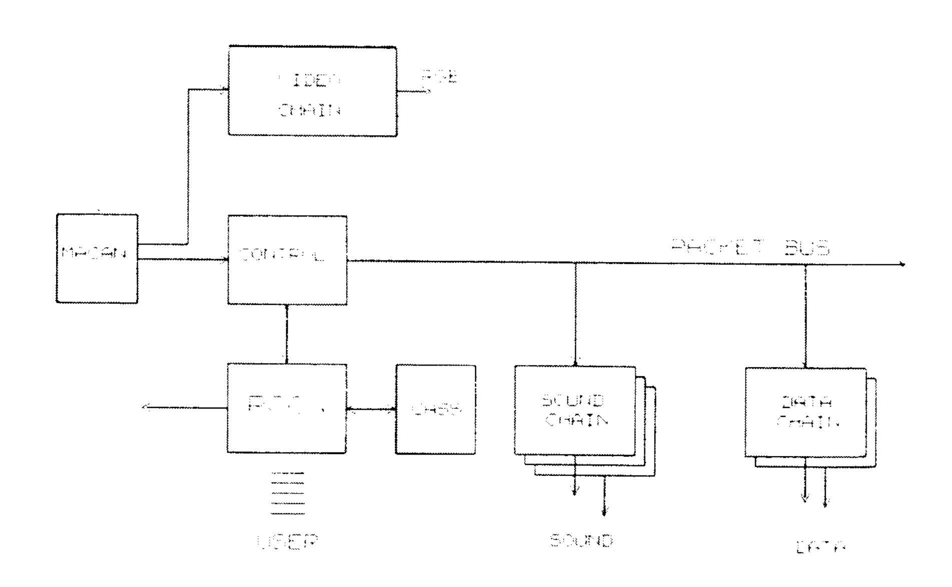


Figure 6. Multi-MAC receiver.
A number of sound
and data services

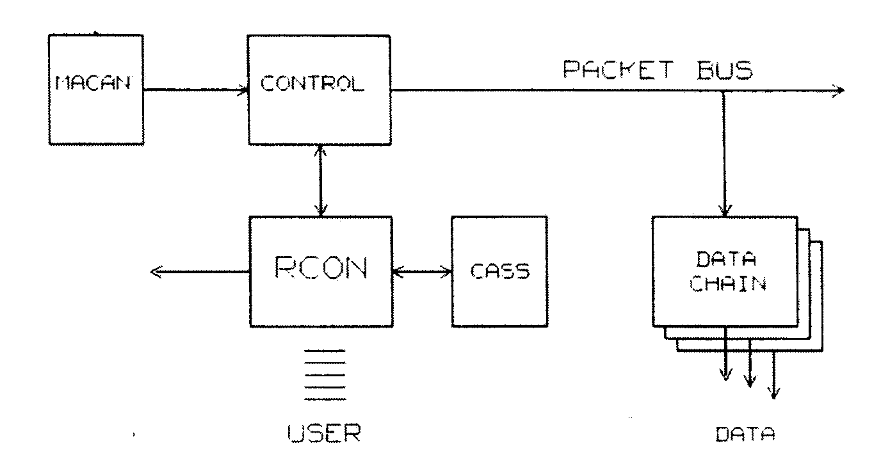


Figure 7. MAC data receiver.
Full-field data, 20 Mbits/sec

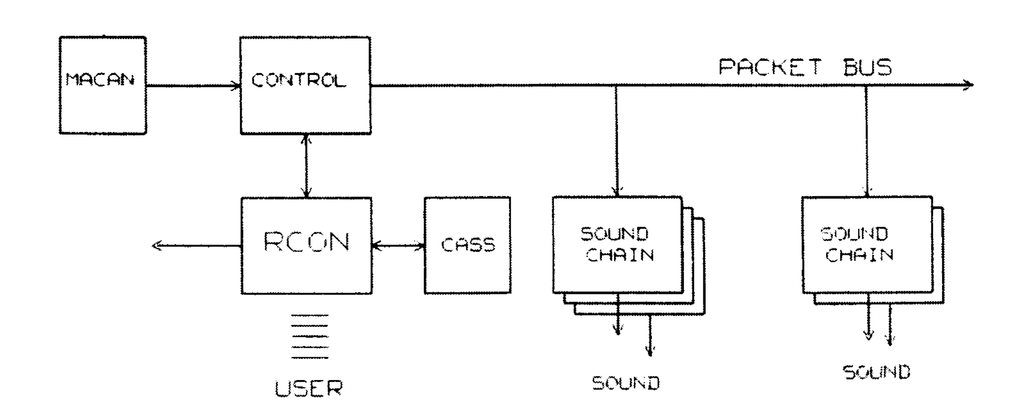


Figure 8. MAC radio receiver.
Up to 48 radio channels

LE POINT DE CODAGE/MULTIPLEXAGE
D2 MAC/PAQUET-EUROCRYPT DE TDF

Philippe **MEILLAN**
Télédiffusion de France
21-27 rue Barbès
92120 MONTROUGE
FRANCE
Tél : +33 (1) 49 65 19 68

RÉSUMÉ

Dans son centre d'exploitation de Romainville TDF a installé le point de codage-multiplexage du système de diffusion par satellite TDF1/TDF2. Ce point de codage permet de coder les signaux alimentant quatre canaux du satellite.
Le centre reçoit les signaux de programme et des données de commande. Les équipements de codage constituent le multiplex D2-MAC final. Les opérateurs disposent de moyens de contrôle et de supervision.
L'attribution de 3 canaux du satellite à des chaînes à accès conditionnel a nécessité une adaptation du point de codage réalisée en dotant d'abord les codeurs existants des organes "contrôleur des titres d'accès" et "injecteur de messagerie" puis en mettant en place une deuxième génération de codeurs intégrant directement ces fonctionnalités.

ABSTRACT

In its Romainville operation center TDF has set up the coding-multiplexing point for TDF1/ TDF2 satellite broadcasting system. This coding center is able to encode four channels on the satellite.
The operation center gathers the programme signals and control data. The encoding equipments build the final D2-MAC multiplex. The staff can use different control means.
As three channels on the satellite are dedicated to condtional access programmes, it became necessary to update the encoding center. As a first step "entitlement controller" and "message injector" have been added to the existing encoders then second generation encoders have been set up. These encoders directly incorporate conditional access facilities.

TABLE DES MATIÈRES

LE POINT DE CODAGE-MULTIPLEXAGE D2-MAC/PAQUET EUROCRYPT

Si l'on examine quels sont les principaux constituants de la chaîne technique d'un système d'accès conditionnel aux programmes audiovisuels tel qu'EUROCRYPT, on peut citer :

- un système de gestion commerciale de la clientèle, mis en oeuvre par l'opérateur de programmes,

- un gestionnaire des titres d'accès, outil technique de la gestion des titres d'accès,

- un point d'émission mis en oeuvre par le radiodiffuseur,

- et bien entendu, les terminaux de réception des usagers.

Les fonctions essentielles du point d'émission sont les suivantes :

- pour ce qui concerne le codage D2-MAC/PAQUET :
codage MAC de l'image,
codage du son,
multiplexage par paquets des sons des données,
multiplexage temporel de l'image, des paquets, du télétexte, ...
gestion des configurations du multiplex,

- pour ce qui concerne l'accès conditionnel EUROCRYPT :
embrouillage de l'image, du ou des sons (des données),
génération et diffusion des messages de contrôle des
titres d'accès, diffusion des messages de gestion des titres d'accès,
gestion des conditions d'accès.

Le point d'émission du système de radiodiffusion par satellite TDF1/ TDF2 a été installé par TDF dans son centre d'exploitation de Romainville. Après avoir rappelé la structure de ce point d'émission (1), nous en décrivons l'adaptation à l'accès conditionnel EUROCRYPT choisi en France et mis en oeuvre sur le système TDF1/ TDF2.

1 - Le point de codage-multiplexage D2 MAC/PAQUET de TDF.

Le point de codage-multiplexage D2 MAC/PAQUET de TDF est équipé pour gérer le codage de 4 chaînes de programme.

Ainsi qu'il est usuel dans un centre d'exploitation de radiodiffusion, le point de codage-multiplexage comporte une salle d'équipements et une régie de commande et de supervision.

1.1. Les équipements

1.1.1. Les interfaces

Le point de codage-multiplexage reçoit des opérateurs de programme les signaux de programme et des données de commande.

Les signaux de commande sont acheminés par des liaisons de contribution conventionnelles sous la forme suivante :

- signal de télévision : signal en composantes analogiques multiplexées (signal T-MAC),

- signaux sonores : multiplex numérique MIC livré sur interface audio-numérique UER-AES,

- signaux de télétexte et de sous-titrage :transportés en suppression de trame du signal T-MAC,

- messages de gestion des titres d'accès : livrées par le Gestionnaire des Titres d'Accès sur liaison X 25.

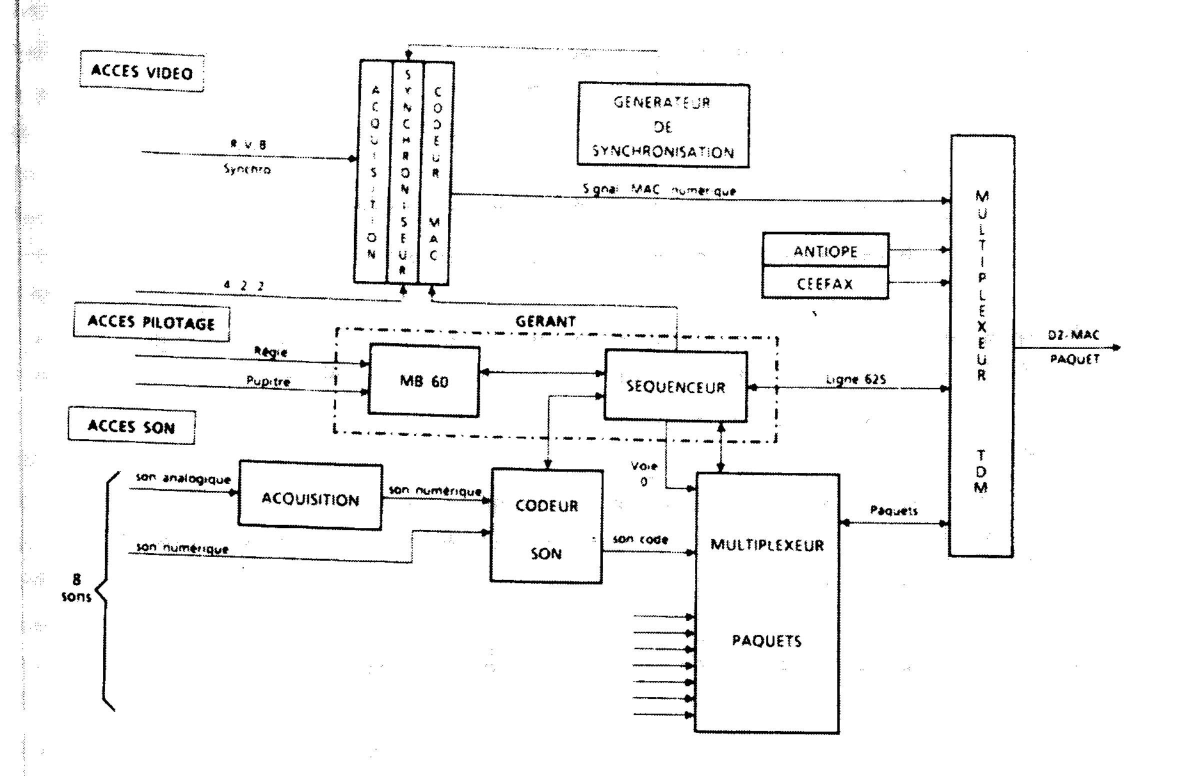
L'opérateur de programme dispose, connecté au codeur D2MAC/PAQUET, d'un poste Opérateur Distant qui permet de définir les configurations du multiplex et de fournir les consignes d'accès conditionnel.

Le signal D2-MAC/PAQUET sortant est acheminé par liaisons de transport de diffusion vers la station de connexion au satellite.

1.1.2.Le codage

Les signaux sont traités et multiplexés par des codeurs D2 MAC/ PAQUET en configuration 1 + 1 ce qui permet d'assurer une disponibilité maximale du signal.

Le schéma ci-dessous permet de rappeler la constitution générale d'un codeur. Les différents blocs fonctionnels correspondent à des équipements individualisés dans la première génération de codeurs acquispar TDF pour assurer les premiers mois (ou années) de l'exploitation au D2-MAC/PAQUET du système TDF1 - TDF2. Dans la génération suivante en cours de démarrage opérationnel, ils constituent des éléments d'une architecture intégrée.



1.2 Le contrôle et la supervision

De manière classique, les opérateurs disposent de moyens de contrôle visuels et auditifs des signaux pris en charge, des signaux codés et d'un retour antenne qui, dans le cas des programmes à conditions d'accès,permettra le contrôle du signal désembrouillé.

Les opérateurs du point de codage-multiplexage disposent de la possibilité de configurer les chaînes de codage et ont la responsabilité d'assurer et de contrôler le partage du canal entre les services cohabitants (services radio et télévision par exemple).

Des moyens de supervision permettent le contrôle permanent du multiplex.En particulier, un gérant d'alarme chaîne vérifie la cohérence entre les consignes fournies par les terminaux d'exploitation et Postes Opérateurs Distants et le contenu du multiplex final.

2 - L'adaptation de l'accès conditionnel.

La mise en oeuvre de l'accès conditionnel selon la norme EUROCRYPT suppose de gérer les voies ECM et EMM transportant respectivement les messages de contrôle et de gestion des titres d'accès.

Ceci conduit à doter les codeurs des organes ou des blocs fonctionnels suivants :

- le contrôleur des titres d'accès

- l'injecteur de messagerie

2.1. Le contrôleur des titres d'accès.

Il génère les messageries de contrôle des titres d'accès.

Rappelons que la messagerie de contrôle des titres d'accès véhicule d'une part les conditions d'accès au programme (par exemple date et thème, numéro de programme, coût, ...) et d'autre part un cryptogramme du mot de contrôle.

Le contrôleur des titres d'accès reçoit les données relatives aux conditions d'accès des Postes Opérateurs Distants.

Les cryptogrammes des mots de contrôle sont calculés par des "cartes-mères" fournies par les opérateurs de programme ; la "carte-mère" reçoit le mot de contrôle tiré au sort par le contrôleur, met en oeuvre l'algorithme cryptographique et restitue le cryptogramme.

Ainsi l'algorithme cryptographique n'est pas connu de l'équipement de codage et lui est inaccessible ce qui renforce de manière considérable la sécurité du système.

L'introduction du contrôle d'accès oblige à revoir la conception de la redondance du système. Dans un codeur D2-MAC/PAQUET "clair" les deux codeurs d'une configuration redondée 1+1 fonctionnent certes avec les mêmes consignes d'exploitation mais de manière indépendante, l'opérateur choisissant le codeur à l'antenne.

L'accès conditionnel, par contre, implique qu'une commutation de codeur ne puisse entraîner de discontinuité dans le désembrouillage par les équipements de réception. De ce fait les deux codeurs d'une configuration redondée doivent en permanence utiliser le même mot de contrôle. Ceci conduit à exploiter les contrôleurs des titres d'accès selon la méthode maître-esclave : le mot de contrôle est tiré par un contrôleur et communiqué à l'autre, le statut des 2 contrôleurs pouvant être permuté en cas de besoin.

2.2. Le diffuseur injecteur de messagerie

Cet équipement assemble et gère les cycles de diffusion des messageries de gestion des titres d'accès.

Le point de codage-multiplexage reçoit un interface supplémentaire (liaison X 25) avec le gestionnaire des titres d'accès qui fournit les messageries de gestion des titres d'accès et leurs consignes de diffusion.

Ces consignes sont :

- la cadence de diffusion des messageries,

- leur période de diffusion (par exemple un message de renouvellement d'abonnement pourra être diffusé un mois),

- le nombre minimal de diffusions du message

- la priorité de diffusion, certains messages requièrent une priorité plus élevée (par exemple le renouvellement d'abonnement sur appel de l'usager).

Pour constituer le cycle de diffusion des messageries l'injecteur tient compte de ces consignes et du débit alloué à la voie numérique de gestion des titres d'accès. Cette voie constitue un des services se partageant le canal (le service d'adressage sur antenne). La diffusion de la messagerie de gestion des titres d'accès suppose de réserver une ressource suffisante à ce service, à côté par exemple des services radio ou des sons du service de télévision. C'est donc un élément à prendre en compte dans le partage du canal.

2.3. L'évolution du point de codage-multiplexage

L'adjonction de ces nouvelles fonctionnalités s'est d'abord effectuée en dotant les codeurs de première génération exploités par TDF des organes "Contrôleur des Titres d'Accès" et "Injecteur de messagerie" avec des possibilités réduites au mode abonnement.

C'est ainsi qu'à pu être assuré dès le 27 mars 1990 la montée de Canal + sur TDF1.

Parallèlement TDF met en place la deuxième génération de codeurs D2 Mac/Paquet développée par MATRA COMMUNICATION et offrant l'ensemble des fonctionnalités du standard EUROCRYPT.

Dans le même temps l'adaptation des moyens de contrôle et de supervision des messageries d'accès conditionnel a été entreprise.

(1) D. DUBOIS, M. GIOVACHINI, Chaîne de codage D2 MAC/PAQUET, Radiodiffusion Télévision n° 101, 1988, p.18 à 22.

MULTI MAC DECODER/DESCRAMBLER

FOR CONSUMER APPLICATIONS

Manfred **JÜNKE**
ITT INTERMETALL
Hans Bunte Str. 19
7800 FREIBURG
WEST GERMANY
Tél : +49 761 5170

ABSTRACT

This lecture will present a set of components of the DIGIT2000 system from ITT Semiconductors supporting the realisation of a Multi-Mac satellite reciever. The various requirements for reception of a multi-service MAC signal are discussed with respect to the implementation in the chip set. The description will concentrate on the DMA 2280 and the DMA 2285 chip which together handle decoding and descrambling of MAC video, sound and data services. Peripheral devices as well as the system philosophy are also addressed.

L'ÉVALUATION ERGONOMIQUE DES INTERFACES UTILISATEURS DE TÉLÉVISION À PÉAGE

Michel **NAËL**
CCETT
4 rue du Clos Courtel
BP 59
35512 CESSON SEVIGNE Cedex
FRANCE
Tél : +33 99 02 47 64

RÉSUMÉ

Traiter de l'évaluation ergonomique des interfaces utilisateurs de télévision à péage dans le contexte de ces journées peut sembler à certains peu pertinent. Cependant, ce sujet a une importance commerciale et implique des interactions avec les aspects techniques. Si cette évaluation de l'interface utilisateur est essentielle, il est non moins essentiel de veiller à la qualité de la méthodologie de test elle-même. L'exposé montre comment deux méthodes différentes produisent des résultats nettement différents. Quelques conséquences sont tirées de cette étude de cas.

ABSTRACT

Dealing with ergonomic assessment of user interfaces for Pay TV in the context of this conference may appear of little relevance to some people. However, this matter entails marketing issues and interactions with technical aspects. This usability testing is crucial, but the testing method itself is as much crucial. The exposé shows how two different methods produce two different sorts of results. A few consequences of this case study are drawn.

TABLE DES MATIÈRES

1 POURQUOI TRAITER DE CE SUJET DANS CE CONTEXTE ?

1.1 Importance commerciale

La qualité ergonomique des produits est aujourd'hui de plus en plus demandée par les clients, en particulier sur les produits électroniques. Il faut bien constater que cette demande correspond à un accroissement des fonctionnalités offertes sur ces produits qui engendre elle-même souvent un accroissement non moins important de la complexité des interfaces utilisateurs. Si un produit, un magnétoscope par exemple, est difficile à programmer, cela gêne l'utilisateur et non le vendeur ou le fabricant une fois l'appareil vendu. Mais lorsqu'il s'agit d'un terminal d'achat d'émissions de télévision, le problème de la facilité d'usage joue sur les consommations, ce qui constitue un argument tout à fait crucial pour la réussite commerciale du service.

1.2 Interactions avec la conception technique

Les concepteurs techniques se représentent souvent les problèmes d'interface utilisateur comme des problèmes qui ne relèvent que des "couches hautes". En disant cela ils pensent que ces problèmes peuvent être traités uniquement à ce niveau et, par conséquent, dans les dernières phases du développement. Sans entrer ici dans trop de détails, notons deux exemples où les caractéristiques du système ont une incidence directe sur l'interface utilisateur.

Ainsi, par exemple, dans l'état actuel du système, il est impossible de "dater" certains achats d'émissions à l'unité. Cela rendra la vérification des factures papier, que l'utilisateur recevra tôt ou tard, plus compliquée que la vérification d'un extrait de compte bancaire habituel en interdisant une recherche par date quel que soit le mode d'achat.

Cet exemple ne peut pas être compensé aujourd'hui au simple niveau du dialogue utilisateur car son origine se trouve dans la définition du système lui-même. Le fait que ce problème soit souligné par les évaluations ergonomiques contribue actuellement à motiver l'étude de certaines modifications de traitement des informations par le désembrouilleur. Le problème du datage de tous les achats sera donc, peut-être, résolu prochainement. Mais il faut retenir de cet exemple que c'est dès le stade des spécifications techniques du système qu'il aurait fallu prendre en compte les effets potentiels sur l'interface utilisateur.

1.3 Dissiper quelques malentendus

Afin d'éviter des confusions et des déceptions, il apparaît utile, tant pour les concepteurs techniques que pour les responsables de marketing, ou même d'autres spécialistes en sciences humaines, de bien distinguer ce que sont des tests d'ergonomie, leur portée et leurs limites. Ceci amènera à passer par l'explicitation et l'illustration de caractéristiques méthodologiques propres à l'ergonomie.

2 L'INTERFACE UTILISATEUR DE TELEVISION A PEAGE

2.1 Entre l'utilisateur et son plaisir télévisuel

Dans le cas de la télévision à péage, l'interface utilisateur est complexe et repose sur trois supports: la télécommande, le coffret et sa carte à mémoire, l'écran du téléviseur. Sur ces supports, apparaissent des informations fixes, telles que les touches et leurs libellés, ou dynamiques, telles que les écrans de dialogue ou les voyants lumineux sur le coffret. Il est courant de considérer le mode d'emploi également comme l'un des éléments de

l'interface utilisateur. Mais l'expérience, et plusieurs études, nous ont montré qu'il est illusoire de penser qu'une difficulté de dialogue peut trouver sa réponse dans le recours au mode d'emploi, car ils sont très souvent mal conçus et très généralement inutilisés. Dans le cas qui nous intéresse ici, l'attention a été portée essentiellement sur la télécommande et sur les interactions qu'elle permet avec un affichage incrusté dans l'écran du téléviseur.

2.2 Distinguer et évaluer tous les niveaux de l'interface

Plusieurs niveaux de l'interface utilisateur doivent être considérés, à titre d'exemples:

	sur la télécommande	sur l'écran TV
niveau physique	forme et feed-back tactile des touches,	contrastes colorés optimisés pour une lisibilité confortable (y compris population âgée ...),
niveau lexical et pictographique	libellé des touches, pictogrammes (très généralement incompris ou mal compris ! ...),	tous les termes utilisés dans les écrans,
niveau syntaxique	répartition, organisation des blocs de touches par groupes fonctionnels,	cohérence des procédures de de confirmation, feed-backs des des actions immédiates et des programmations, ...
niveau sémantique	compréhension et mémorisation de la signification des touches,	cohérence du dialogue avec les buts et les habitudes des usagers,

Des interrelations existent évidemment entre ces différents niveaux. Ainsi, par exemple, la mémorisation de la signification des touches de la télécommande dépend de son libellé, de sa position par rapport aux autres touches et de marquages graphiques ou colorés. C'est donc l'ensemble de ces niveaux qui doivent être évalués.

3 COMMENT EVALUER CET INTERFACE ?

3.1 Les pratiques courantes en tests de produit

Les services de marketing ont souvent recours à des tests de produits, soit existants soit nouveaux, afin d'évaluer leur attrait pour les clients potentiels. Dans le cas d'un produit nouveau, il s'agit notamment d'avaluer si le concept même du produit est bien perçu et apprécié positivement. Les techniques mises en œuvre reposent essentiellement sur des entretiens et sur des jeux de rôles. L'analyse qui est faite porte sur le discours des panélistes. Un accent particulier est mis sur la représentation idéale que les panélistes se font du produit.

3.2 Caractéristiques des tests d'ergonomie

Les tests d'ergonomie présentent, pour leur part, des caractéristiques sensiblement différentes des tests de produits, même si l'interview des panélistes y joue aussi un rôle important:

- l'objectif est d'évaluer la compatibilité de l'interface avec les buts, les capacités et les habitudes des utilisateurs, et non pas les aspects plus ou moins séduisants du produit,

- la référence essentielle est "l'utilisateur réel en situation réelle", ce qui nécessite pour un produit nouveau, au moyen du maquettage et des scénarios de tests, un effort important pour créer une situation aussi réaliste que possible, (*)

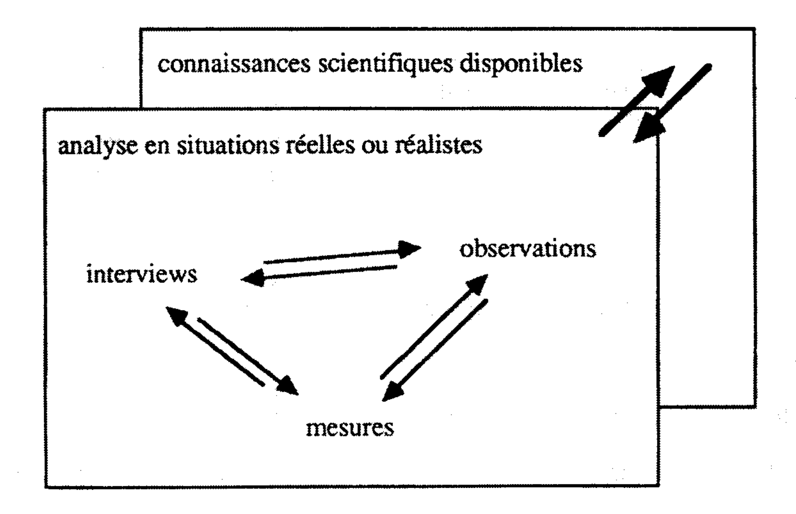
- le scénario de tests comporte donc nécessairement une phase où un ensemble de tâches sont proposées aux panélistes (par exemple: "programmer Visiopass si l'on veut enregistrer une émission que l'on ne pourra regarder au moment de la diffusion sur tel chaîne, tel jour, de telle heure à telle heure"), tâches qu'ils ont à réaliser seuls, dans l'ordre qui leur convient, sans aide autre que le dialogue utilisateur lui-même,

- les données recueillies sont des observations comportementales (les panélistes parviennent-ils aux buts qui leurs sont proposés, et de quelle façon ?), des verbalisations (des difficultés rencontrées, des opinions aussi ...) et des quantifications (temps mis pour atteindre tel objecitf, nombre d'hésitations ou d'erreurs, etc.),

- il est important de souligner qu'un type de donnée doit être confrontée, autant que possible, à un autre type de donnée; ainsi, aux opinions exprimées, il faut chercher des validations dans les comportements observés,

- lorsqu'il en existe, le recours à des connaissances scientifiques est également nécessaire, par exemple pour argumenter sur des problèmes de lisibilité (contrastes colorés, taille des caractères, ...),

Résumons ces caractéristiques dans le schéma suivant:



Les données recueillies se situent au-delà des "opinions"

(*) Le dialogue utilisateur, dans ce cas comme souvent, est le résultat de nombreuses contributions qu'il serait trop long de citer ici. Il faut cependant mentionner qu'au CCETT, le maquettage du dialogue et la simulation des interactions avec un programme audiovisuel diffusé est le résultat d'un travail important de programmation informatique (Yves HERVET en grande partie, et Christian GERARD). Les tests d'ergonomie n'ont de sens et d'utilité qu'en s'appuyant sur la réalisation du maquettage, et de ses nombreuses modifications en cours d'étude.

4 LES RESULTATS OBTENUS

4.1 Deux méthodologies d'évaluation différentes

Dans le cas qui nous intéresse, deux maquettes de dialogue utilisateur pour Visiopass ont été évaluées, l'une réalisée par un industriel, l'autre par le CCETT (*). Ces deux maquettes présentaient globalement les mêmes caractéristiques de dialogue, notamment: même structure des menus, même terminologie (à quelques détails près). La maquette réalisée au CCETT présentait un aspect de réalisme supplémentaire dans la mesure où certaines actions étaient possibles avec un programme audiovisuel embrouillé/désembrouillé.

Deux prestataires de services différents ont évalué ces maquettes. Appelons "A" celui qui a évalué la maquette de l'industriel et "B" celui qui a évalué la maquette du CCETT. La méthodologie suivie a été sensiblement différente dans les deux cas, notamment sur les points suivants:

- le prestataire A, praticien expérimenté en tests de produits a centré, presque exclusivement, son évaluation sur les interviews (son protocole de test s'intitule d'ailleurs "guide d'entretien"); le déroulement du test se faisait en présence continue de l'interviewer, selon la démarche suivante: explication d'une rubrique, proposition d'un "exercice" sur cette rubrique, et interview simultané,

- le prestataire B, praticien expérimenté en tests d'ergonomie, a réalisé ses tests en respectant les caractéristiques mentionnées au point 3.2, en particulier pour la phase durant laquelle les panélistes se trouvent seuls face au système.

D'autres différences méthodologiques, telles que la passation d'un panéliste seul (prestataire A) ou plutôt par paires de personnes qui se connaissent (prestataire B) pour faciliter les verbalisations et réduire l'aspect artificiel de la situation du test, distinguaient également les deux prestataires.

4.2 La méthode conditionne les résultats

La différence méthodologique décrite précédemment peut sembler bien négligeable à certains, même à des spécialistes d'autres sciences humaines ... Pourtant, il s'avère que cette différence a entraîné des conséquences sensibles sur les résultats:

- dans un parcours imposé du dialogue et rubrique par rubrique (prestataire A), il était évidemment impossible de trouver des informations (comportementales et/ou verbales) sur les difficultés potentielles des panélistes pour se repérer dans la logique et la structure globales du dialogue; en conséquence, dans les recommandations, il n'est pas surprenant qu'un accent important ait été mis sur des points tels que l'utilisation du curseur pour choisir entre plusieurs options, et qu'il n'y ait pratiquement pas de recommandation pour améliorer la structure et du dialogue lui-même,

- dans les scénarios où les panélistes se sont trouvés seuls face à l'ensemble du dialogue et devant remplir des tâches proposées (prestataire B), les possibilités d'erreurs, et d'errance, dans le dialogue ont pu se manifester; ainsi sont apparues des confusions que les panélistes faisaient entre ce qu'ils pouvaient consulter et ce sur quoi ils pouvaient agir, entre ce qui relève du système (le coffret et la carte) et ce qui relève de "la chaîne

---

(*) Pour une description fonctionnelle complète du désembrouilleur VISIOPASS, consulter l'article de G. DUVIC et C. GEOFFRAY, publié dans ce même document.

qu'ils regardent"; ces confusions gênent l'utilisation complète des fonctions et freinent son appropriation par les utilisateurs. On voit bien qu'il s'agit là d'un problème d'une autre dimension que celui, pourtant réel aussi, de l'apprentissage de modalités de désignation non familières mais très vite acquises.

Les deux prestataires ont bien souligné la complexité ressentie par les panélistes. Mais le prestataire B a pu en faire une analyse plus fine et plus exacte, qui nous a permis de remettre en cause l'organisation générale du dialogue. Bien qu'il ne s'agit pas là d'une comparaison strictement expérimentale, nous avons donné quelques raisons de penser que la qualité des résultats tient en grande partie aux différences de la méthodologie et du champ de compétence des évaluateurs.

4.3 Portée et limites des tests d'ergonomie

Dans cest tests, quelle que soit leur qualité, il ne faut jamais oblier quelques limites:

- "réaliste" n'est pas "réel", de nombreuses dimensions de la réalité manquent toujours, tels que l'environnement domestique familier, et, dans ce cas, la dimension financière du rapport au produit ...; de plus, un maquettage est toujours, plus ou moins, incomplet (dans notre cas, par exemple, il était impossible de présenter un fonctionnement très réaliste, c'est à dire avec feed-back sonore, de la fonction "mixage des sons", ou du service radio évidemment ...),

- l'ergonomie d'un produit n'est que l'un des facteurs d'acceptabilité, l'utilité ressentie et le coût du produit/service offert jouent souvent un rôle plus important dans sa réussite commerciale.

5 QUELQUES CONCLUSIONS

5.1 Il y a vraiment "test" et "test" ...

La pratique des tests d'usage semble se développer et il faut s'en féliciter. Nous avons voulu montrer, pour des interlocuteurs qui peuvent ignorer ces "subtilités", que l'on n'obtient pas les mêmes types de résultats selon la méthodologie mise en œuvre. Les tests visant à évaluer les motivations d'achat d'un produit ou d'un service ont leur utilité et leur pertinence dans une perspective d'étude de marché. Pour améliorer la qualité de l'interface utilisateur, il est plus utile et pertinent de recourir à des tests d'ergonomie qui n'en portent pas seulement le nom.

5.2 L'articulation entre ergonomie et processus de développement

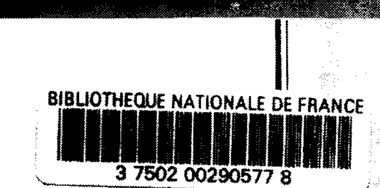
Il apparaît nécessaire d'intégrer les tests d'ergonomie aussitôt que possible dans le processus de conception. Cela est possible dès le stade de la définition des spécifications fonctionnelles. En effet, si le concepteur peut décrire le fonctionnement externe du produit, alors un maquetteur peut déjà lui donner des formes réalistes pour des utilisateurs potentiels. Les premiers maquettages sont nécessairement rudimentaires, l'important est qu'ils soient interactifs, de façon à permettre aux panélistes de réaliser, par eux-mêmes, des séquences d'actions suffisamment représentatives de l'utilisation future probable.

De plus, la réalité des processus de conception et développement montre que:
- aucun dialogue utilisateur n'a été "réussi" du premier coup,
- de nombreux aléas techniques se présentent aussi en cours de développement.

Ces deux raisons justifient une démarche itérative entre des phases de maquettages, d'évaluations et de modifications successives, démarche qui est, en fait, la seule qui soit réaliste.

Enfin, l'intégration précoce d'évaluations ergonomiques dans le processus de conception contribue à limiter, autant pour les concepteurs que pour les ergonomes, le syndrôme de "l'inspecteur des travaux finis". Cela contribue aussi à construire un langage commun entre ergonome et concepteur (de bonne foi l'un et l'autre ...), condition nécessaire pour que la collaboration soit fructueuse.

 ISBN 2-906850-03-9
Groupe Media Calligraphy 99 26 72 72
Dépôt Légal 2° trimestre 1990



Actes des Premières Journées Internationales ACSA'90

Accès Conditionnel aux Services Audiovisuels/*Conditional Access for Audiovisual Services*

RENNES
12-13-14 juin 1990
France